(19) KOREAN INTELLECTUAL PROPERTY OFFICE

KOREAN PATENT ABSTRACTS

(11)Publication number: 1020000029092 A
(43)Date of publication of application: 25.05.2000

(21)Application number: 1019990044669
(22)Date of filing: 15.10.1999
(30)Priority: 16.10.1998 JP 98 295920
30.11.1998 JP 98 339027

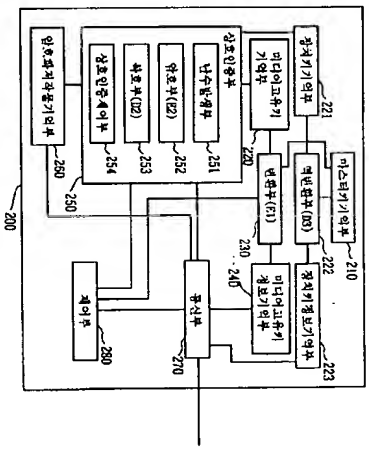
(51)Int. Cl G09C 1/00

(71)Applicant: MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD.

(72)Inventor: HARADA SUNJI
KOZUKA MASAYUKI
NAKAMURA YUTAKA
TATEBAYASHI MAKOTO

(54) PROTECTING SYSTEM FOR DIGITAL WORKS

(57) Abstract:



PURPOSE: A system is provided to prevent digital works such as digitalized writing, sound, image, or program from being recorded and replayed illegally.

CONSTITUTION: A memory unit(220) of media inherent key memorizes one inherent key Ki for a converting unit(230) to generate a ciphered inherent key Ji from the inherent key Ki. Also, a generating unit of random number generates a random number R1, a cipher unit(252) generates a ciphered random number S1 from the random number R1 and a decoding unit generates a random number R'1 from the ciphered random number S1. And, a controller of certifying firm name compares the random number R'1 with the random number R1 for certifying a writer of memory card having a memory card (200) and a decipherer of memory card as regal apparatuses in case of identity of the random numbers. And then, the writer and the decipherer of memory card code or decode the works by using the decoded inherent key.

COPYRIGHT 2000 KIPO

Legal Status
Date of final disposal of an application (00000000)
Patent registration number ( )
Date of registration (00000000)
Number of opposition against the grant of a patent ( )
Date of opposition against the grant of a patent (00000000)
Number of trial against decision to refuse ( )
Date of requesting trial against decision to refuse ( )
Date of extinction of right ( )

BEST AVAILABLE COPY

(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(51) Int. Cl.[7]
G09C 1/00

(11) 공개번호 특2000-0029092
(43) 공개일자 2000년05월25일

(21) 출원번호 10-1999-0044669
(22) 출원일자 1999년10월15일
(30) 우선권주장 특원평10-295920 1998년10월16일 일본(JP)
특원평10-339027 1998년11월30일 일본(JP)
(71) 출원인 마츠시타 덴끼 산교 가부시키가이샤
일본 오오사카후 가도마시 오오아자 가도마 1006
(72) 발명자 다테바야시마코토
일본국효고켄다카라즈카시메후1-16-21
나카무라유타카
일본국교토후교토시후시미쿠무카이지마니노마루쵸151-30-3-1109
하라다순지
일본국오오사카후오오사카시니시나리쿠다마데니시2-20-52
고즈카마사유키
미합중국캘리포니아아카디아코일애비뉴501
(74) 대리인 김영철

심사청구 : 없음

(54) 디지털 저작물 보호시스템

요약

미디어고유키 기억부(220)는 미리 하나의 고유키 Ki를 기억하고, 변환부(230)는 판독한 고유키 Ki로부터 암호화 고유키 Ji를 생성하며, 난수발생부(331)는 난수 R_1을 생성하고, 암호부(252)는 난수 R_1로부터 암호화난수 S_1을 생성하고, 복호부(333)는 암호화난수 S_1로부터 난수 R'_1을 생성하고, 상호인증 제어부(334)는 난수 R'_1과 난수 R_1을 비교하여 일치하면 메모리카드(200)가 장착된 메모리카드 기입기, 메모리카드 판독기가 정당한 장치라고 인증한다. 메모리카드와 메모리카드 기입기 또는 메모리카드 판독기가 서로 정당한 장치라고 인증된 경우, 메모리카드 기입기 또는 메모리카드 판독기는 복호한 고유키를 이용하여 저작물을 암호 또는 복호한다.

대표도

도1

명세서

도면의 간단한 설명

도 1은 본 발명에 관한 하나의 실시예로서의 디지털 저작물 보호시스템(100)의 블록도

도 2는 메모리카드(200)가 메모리카드 기입기(300)에 장착되고, 메모리카드 기입기(300)가 퍼스널 컴퓨터(500)에 장착되는 상태도

도 3은 메모리카드(200)가 메모리카드 판독기(400)의 일종인 헤드폰 스테레오(401)에 장착되는 상태도

도 4는 메모리카드(200)의 구성을 도시한 블록도

도 5는 메모리카드 기입기(300)의 구성을 도시한 블록도

도 6은 메모리카드 판독기(400)의 구성을 도시한 블록도

도 7은 메모리카드(200)가 메모리카드 기입기(300)에 장착된 경우의 개요동작을 도시한 흐름도

도 8은 메모리카드(200)가 메모리카드 판독기(400)에 장착된 경우의 개요동작을 도시한 흐름도

도 9는 메모리카드(200)가 메모리카드 기입기(300)에 장착된 경우의 상호의 상세한 인증동작도

도 10은 메모리카드(200)가 메모리카드 기입기(300)에 장착된 경우의 메모리카드 기입기(300)가 메모리카

드(200)를 인증하는 동작도

도 11은 본 발명에 관한 또 다른 실시예의 하나로서의 디지털 저작물 보호시스템(100a)의 구성을 도시한 블록도

도 12는 메모리카드(200a)가 미디어 고유키 정보작성장치(600)에 장착된 경우의 동작 및 메모리카드(200a)가 메모리카드 기입기(300)에 장착된 경우의 상세한 인증동작도

도 13은 본 발명에 관한 또 다른 실시예의 하나로서의 디지털 저작물 보호시스템에 있어서, 메모리카드(200)가 메모리카드 기입기(300)에 장착된 경우의 상세한 인증동작도

도 14는 본 발명에 관한 또 다른 실시예의 하나로서의 디지털 저작물 보호시스템(100c)에서의 메모리카드(200c)의 구성을 도시한 블록도

도 15는 디지털 저작물 보호시스템(100c)에서의 메모리카드 기입기(300c)의 구성을 도시한 블록도

도 16은 디지털 저작물 보호시스템(100c)에서의 메모리카드 판독기(400c)의 구성을 도시한 블록도

도 17은 디지털 저작물 보호시스템(100d)의 구성을 도시한 블록도

도 18은 디지털 저작물 보호시스템(100d)의 동작도

도 19는 디지털 저작물 보호시스템(100e)의 구성을 도시한 블록도

도 20은 디지털 저작물 보호시스템(100e)의 인증의 동작도

도 21은 디지털 저작물 보호시스템(100f)의 구성을 도시한 블록도

도 22는 디지털 저작물 보호시스템(100f)의 인증의 동작도

도 23은 디지털 저작물 보호시스템(100g)의 구성도

도 24는 디지털 저작물 보호시스템(100g)의 인증의 동작도

도 25는 디지털 저작물 보호시스템(100h)의 구성도. 도 26에 계속됨

도 26은 디지털 저작물 보호시스템(100h)의 구성을 도시한 블록도. 도 25로부터 계속

도 27은 디지털 저작물 보호시스템(100h)의 동작도. 메모리카드(200)가 메모리카드 기입기(300h)에 장착된 경우의 개요동작도

도 28은 디지털 저작물 보호시스템(100h)의 동작도. 메모리카드(200)가 메모리카드 판독기(400h)에 장착된 경우의 개요동작도

도 29는 디지털 저작물 보호시스템(100i)의 구성을 도시한 블록도. 도 30에 계속됨.

도 30은 디지털 저작물 보호시스템(100i)의 구성을 도시한 블록도. 도 29로부터 계속.

도 31은 디지털 저작물 보호시스템(100i)의 동작도. 메모리카드(200i)가 메모리카드 기입기(300i)에 장착된 경우의 개요동작도

도 32는 디지털 저작물 보호시스템(100i)의 동작도. 메모리카드(200i)가 메모리카드 판독기(400i)에 장착된 경우의 개요동작도

도 33은 디지털 저작물 보호시스템(100i)의 다른 구성을 도시한 블록도.

도 34는 디지털 저작물 보호시스템(100j)의 또 다른 구성을 도시한 블록도

도 35는 메모리카드(200j)가 메모리카드 기입기(300j)에 장착된 경우의 상호의 상세한 인증동작도

발명의 상세한 설명

발명의 목적

발명이 속하는 기술분야 및 그 분야의 종래기술

본 발명은 디지털화된 문서, 음성, 화상, 프로그램 등의 디지털 저작물을 네트워크에서 배포하고, 이것을 기억매체에 기록하고, 플레이어로 재생하는 시스템에 관한 것으로, 특히 부정하게 이들의 기록이나 재생이 행해지는 것을 방지하는 시스템에 관한 것이다.

최근 디지털화된 문서, 음성, 화상, 프로그램 등의 디지털 저작물이 인터넷등의 네트워크를 경유하여 유통되고, 이용자는 여러가지 디지털 저작물을 간단히 네트워크를 경유하여 인출하여 다른 기록매체에 기록하고, 재생할 수 있게 되었다.

발명이 이루고자 하는 기술적 과제

그러나 이와 같이 간단히 디지털 저작물을 복제할 수 있다는 이점은 있지만, 저작자의 저작권이 침해되기 쉽다는 문제점이 있다.

본 발명은 외부로부터 인출된 디지털 저작물을 부정하게 기록매체에 기입하는 것과, 기록매체에 기록된 디지털 저작물을 부정하게 재생하는 것을 방지하는 디지털 저작물 보호시스템, 디지털 저작물 보호방법, 기록매체에 기록되어 있는 디지털 저작물 보호프로그램 및 통신회선을 통해 전송되는 디지털 저작물 보호

프로그램을 제공하는 것을 목적으로 한다.

발명의 구성 및 작용

상기 목적을 달성하는 디지털 저작물 보호시스템은 디지털 저작물정보를 기억하는 영역을 갖는 기록매체장치와, 상기 영역으로부터 정보를 판독 또는 상기 영역에 정보를 기입하는 액세스장치로 구성되고, 상기 기록매체장치와 상기 액세스장치 사이에서 디지털 저작물의 이용을 실현하는 디지털 저작물 보호시스템에 있어서, 상기 기록매체장치는 소유하는 고유키를 상기 액세스장치에 비밀 전송하고, 상기 기록매체장치 및 상기 액세스장치는 각각 상기 고유키를 이용하여 상대 장치의 정당성을 인증하는 단계로서, 상기 고유키는 상기 기록매체장치에 고유한 키정보인 인증단계과, 상기 기록매체장치와 상기 액세스장치가 모두 정당성을 갖는다고 인증된 경우에, 상기 액세스장치는 상기 고유키를 이용하여 디지털 저작물을 암호화하여 상기 기록매체장치로 전송하거나 또는 상기 기록매체장치로부터 전송된 암호화된 디지털 저작물을 상기 고유키를 이용하여 복호하는 저작물전송단계를 포함하는 것을 특징으로 한다.

이 구성에 의하면 정당한 장치로부터 부정한 장치로의 저작물의 전송을 방지할 수 있으므로 정당하게 취득된 저작물이 부정하게 이용되는 것을 방지할 수 있는 것과 아울러, 또 부정한 장치로부터 정당한 장치로의 저작물의 전송을 방지할 수 있으므로 부정하게 취득된 저작물을 더 이용하는 것을 방지할 수 있다.

여기에서, 상기 인증단계에서의 상기 액세스장치에 의한 상기 기록매체장치의 정당성 인증에서, 상기 기록매체장치는 제 1 연산수단을 포함하며, 상기 액세스장치는 제 1 인증정보 생성수단과 제 1 인증수단을 포함하며, 상기 제 1 인증정보 생성수단은 제 1 인증정보를 생성하고, 생성한 상기 제 1 인증정보를 상기 기록매체장치에 출력하며, 상기 제 1 연산수단은 상기 제 1 인증정보를 수취하고, 상기 고유키를 이용하여 상기 제 1 인증정보에 제 1 연산을 실시하여 제 1 연산 인증정보를 생성하고, 생성한 상기 제 1 연산 인증정보를 상기 액세스장치에 출력하며, 상기 제 1 인증수단은 비밀전송된 상기 고유키를 이용하며, 상기 제 1 인증정보와, 상기 제 1 연산 인증정보에 의해 상기 기록매체장치가 정당성을 갖는지의 여부를 인증하는 것으로 해도 된다.

상기 인증단계에서의 상기 기록매체장치에 의한 상기 액세스장치의 정당성 인증에서, 상기 액세스장치는 제 2 연산수단을 포함하며, 상기 기록매체장치는 제 2 인증정보 생성수단과 제 2 인증수단을 포함하며, 상기 제 2 인증정보 생성수단은 제 2 인증정보를 생성하고, 생성한 상기 제 2 인증정보를 상기 액세스장치에 출력하며, 상기 제 2 연산수단은 상기 제 2 인증정보를 수취하고, 비밀전송된 상기 고유키를 이용하여 상기 제 2 인증정보에 제 2 연산을 실시하여 제 2 연산 인증정보를 생성하고, 생성한 상기 제 2 연산 인증정보를 상기 기록매체장치에 출력하며, 상기 제 2 인증수단은 상기 고유키를 이용하며, 상기 제 2 인증정보와, 상기 제 2 연산인증정보에 의해 상기 액세스장치가 정당성을 갖는지의 여부를 인증하는 것으로 해도 된다.

이 구성에 의하면, 장치는 접속된 상대의 장치가 정당한 장치인지, 부정한 장치인지를 인증할 수 있다.

상기 인증단계에서의 상기 기록매체장치로부터 상기 액세스장치로의 고유키 비밀전송에서, 상기 기록매체장치는, 상기 고유키를 기억하는 고유키 기억수단과, 상기 고유키에 제 1 암호알고리즘을 실시하여 암호화 고유키를 생성하고, 생성한 상기 암호화 고유키를 상기 액세스장치로 출력하는 제 1 암호수단을 포함하며, 상기 액세스장치는, 상기 암호화 고유키를 수취하고, 상기 암호화 고유키에 제 1 복호알고리즘을 실시하여 복호고유키를 생성하는 제 1 복호수단을 포함하고, 여기에서 상기 제 1 복호알고리즘은 상기 제 1 암호알고리즘에 의해 생성된 암호문을 복호하는 제 1 복호수단을 포함하는 것으로 해도 된다.

이 구성에 의하면 고유키를 암호화하여 기록매체장치로부터 액세스장치로 전송하므로 고유키가 폭로될 가능성이 낮아진다.

여기에서, 상기 제 1 키는 마스터키로서 상기 제 2 키와 동일키이고, 상기 제 2 키는 마스터키이고, 상기 제 1 복호수단은 상기 제 1 키와 동일한 상기 제 2 키를 이용하여 상기 암호화 고유키에 상기 제 1 복호알고리즘을 실시하여 상기 복호고유키를 생성하는 것으로 해도 된다.

이 구성에 의하면 기록 장치와 액세스장치는 동일한 마스터키를 가지므로 기록장치와 액세스장치의 제조가 용이하게 행해진다는 효과가 있다.

여기에서 상기 제 1 키는 상기 제 2 키를 기초로 하여, 공개키 암호방식의 공개키 결정알고리즘에 의해 산출되는 공개키이고, 상기 제 1 암호수단은 상기 제 1 키를 이용하여 상기 고유키에 상기 제 1 암호알고리즘을 실시하여 상기 암호화 고유키를 생성하며, 상기 제 1 암호알고리즘은 상기 공개키 암호방식의 암호알고리즘이고, 상기 제 1 복호수단은 상기 제 2 키를 이용하여 상기 암호화 고유키에 상기 제 1 복호알고리즘을 실시하여 상기 복호고유키를 생성하며, 상기 제 1 복호알고리즘은 상기 공개키 암호방식의 복호알고리즘으로 해도 된다.

이 구성에 의하면, 공개키인 제 1 키와 비밀키인 제 2 키와는 달리 카드 판독기 또는 카드 기입기에 존재하는 비밀키가 가령 폭로되었다고 해도 이제부터 공개키를 구할 수 없으므로 메모리카드의 위조가 어렵다는 효과가 있다.

여기에서 상기 제 2 키는 상기 제 1 키를 기초로 하여 회복형 서명처리방식의 공개키 결정알고리즘에 의해 산출되는 공개키이고, 상기 제 1 암호알고리즘은 상기 회복형 서명처리방식의 서명처리 알고리즘이며, 상기 제 1 암호수단은 상기 제 1 키를 이용하여 상기 고유키에 상기 제 1 암호알고리즘을 실시하여 서명문인 상기 암호화 고유키를 생성하며, 상기 제 1 복호알고리즘은 상기 회복형 서명처리방식의 검증처리알고리즘이며, 상기 제 1 복호수단은 상기 제 2 키를 이용하여 서명문인 상기 암호화 고유키에 상기 제 1 복호알고리즘을 실시하고, 상기 복호고유키를 생성하는 것으로 해도 된다.

이 구성에 의하면, 공개키 K_p로부터 비밀키 K_s를 구하는 것이 계산양적으로 매우 어렵게 된다. 따라서 메모리카드에 비해 내부해석의 위협성이 상대적으로 높다고 생각되는 메모리 기입기 또는 메모리 판독기에 공개키를 부여하고, 메모리카드에 비밀키를 부여하는 구성이 운용시스템 전체의 기밀성을 높인다는 효과

가 있다.

여기에서, 상기 기록매체장치는, 또한 복수개의 마스터키로 된 마스터키군을 미리 기억하고 있는 제 1 마스터키 기억수단과, 상기 마스터키군 중에서 하나의 마스터키를 제 1 키로서 선택하는 제 1 선택수단을 포함하며, 상기 제 1 암호수단은 선택된 상기 제 1 키를 이용하여 상기 고유키에 상기 제 1 암호알고리즘을 실시하여 상기 암호화 고유키를 생성하며, 상기 액세스장치는, 또한 상기 마스터키군과 동일한 마스터키군을 미리 기억하고 있는 제 2 마스터키 기억수단과, 상기 제 2 마스터키 기억수단에 기억되어 있는 마스터키군 중에서 상기 제 1 키와 동일한 마스터키를 제 2 키로서 선택하는 제 2 선택수단을 포함하며, 상기 제 1 복호수단은 상기 제 1 키와 동일한 상기 제 2 키를 이용하여 상기 암호화 고유키에 상기 제 1 복호알고리즘을 실시하여 상기 복호고유키를 생성하는 것으로 해도 된다.

이 구성에 의하면 기록매체 및 액세스장치는 복수의 마스터키를 갖고 있으므로 복수의 다른 디지털 저작물 운용시스템에서도 적용할 수 있다는 효과가 있다.

여기에서, 상기 제 1 암호수단은, 서브그룹키를 미리 기억하고 있고, 상기 서브그룹키를 이용하여 상기 고유키에 제 1 변환을 실시하여 변형키를 생성하며, 상기 변형키에 상기 제 1 암호알고리즘을 실시하여 상기 암호화 고유키를 생성하며, 상기 제 1 복호수단은, 상기 서브그룹키와 동일한 서브그룹키를 미리 기억하고 있고, 상기 암호화 고유키에 상기 제 1 복호알고리즘을 실시하여 복호변형키를 생성하고, 상기 서브그룹키를 이용하여 상기 복호변형키에 상기 제 1 변환의 역변환을 실시하여 복호고유키를 생성하는 것으로 해도 된다.

이 구성에 의하면, 하나의 디지털 저작물 운용시스템을 복수의 단체가 운영하는 경우, 이들의 단체의 수만큼 다른 서브그룹키가 존재하며, 이들의 다른 서브그룹키가 각각 상기 복수의 단체에 할당되므로 각 단체는 독자적인 서비스 제공이 가능해진다. 또 메모리카드의 기억용량은 한정되어 있으므로 메모리카드에 기억할 수 있는 마스터키의 수에는 제한이 있는 경우가 많고, 마스터키와 서브그룹키의 조합에 의해 이용할 수 있는 키의 수를 늘릴 수 있다는 효과가 있다.

여기에서, 상기 제 1 암호수단은, 서브그룹키를 미리 기억하고 있고, 상기 고유키에 제 1 암호알고리즘을 실시하여 암호문을 생성하고, 상기 서브그룹키를 이용하여 상기 암호문에 제 1 변환을 실시하여 암호화 고유키를 생성하며, 상기 제 1 복호수단은, 상기 서브그룹키와 동일한 서브그룹키를 미리 기억하고 있고, 상기 서브그룹키를 이용하여 상기 암호화 고유키에 상기 제 1 변환의 역변환을 실시하여 복호문을 생성하고, 상기 복호문에 상기 제 1 복호알고리즘을 실시하여 복호고유키를 생성하는 것으로 해도 된다.

이 구성에 의하면 하나의 디지털 저작물 운용시스템을 복수의 단체가 운영하는 경우, 상기와 같이 각 단체는 독자적인 서비스 제공이 가능해진다. 또 마스터키와 서브그룹키의 조합에 의해 이용할 수 있는 키의 수를 늘릴 수 있다는 효과가 있다.

여기에서, 상기 기록매체장치는 또한 제 1 키를 미리 기억하고 있는 제 1 키 기억수단을 포함하며, 상기 제 1 키는 마스터키이며, 상기 제 1 암호수단은, 서브그룹키를 미리 기억하고 있고, 상기 서브그룹키를 이용하여 상기 제 1 키에 제 1 변환을 실시하여 암호화 제 1 키를 생성하고, 생성한 상기 암호화 제 1 키를 이용하여 상기 고유키에 상기 제 1 암호알고리즘을 실시하여 상기 암호화 고유키를 생성하며, 상기 액세스장치는 또한 제 2 키를 미리 기억하고 있는 제 2 키 기억수단을 포함하며, 상기 제 2 키는 마스터키로서 상기 제 1 키와 동일키이고, 상기 제 1 복호수단은, 상기 서브그룹키와 동일한 서브그룹키를 미리 기억하고 있고, 상기 서브그룹키를 이용하여 상기 제 2 키에 상기 제 1 변환과 동일한 변환을 실시하여 암호화 제 2 키를 생성하고, 생성한 상기 암호화 제 2 키를 이용하여 상기 암호화 고유키에 상기 제 1 복호알고리즘을 실시하여 상기 복호고유키를 생성하는 것으로 해도 된다.

이 구성에 의하면, 하나의 디지털 저작물 운용시스템을 복수의 단체가 운영하는 경우, 상기와 같이 각 단체는 독자적인 서비스 제공이 가능해진다. 또 마스터키와 서브그룹키의 조합에 의해 이용할 수 있는 키의 수를 늘릴 수 있다는 효과가 있다.

여기에서, 상기 제 1 연산수단은, 서브그룹키를 미리 기억하고 있고, 상기 서브그룹키를 이용하여 상기 고유키에 제 1 변환을 실시하여 변형고유키를 생성하며, 생성한 상기 변형고유키를 이용하여 상기 제 1 인증정보에 상기 제 1 연산을 실시하여 상기 제 1 연산인증정보를 생성하며, 상기 제 3 연산수단은, 상기 서브그룹키와 동일한 서브그룹키를 미리 기억하고 있고, 상기 서브그룹키를 이용하여 비밀전송된 상기 고유키에 상기 제 1 변환의 역변환을 실시하여 변형복호 고유키를 생성하고, 생성한 상기 변형복호 고유키를 이용하여 상기 제 1 인증정보에 상기 제 1 연산과 동일한 연산을 실시하여 상기 제 3 연산인증정보를 생성하는 것으로 해도 된다.

이 구성에 의하면, 하나의 디지털 저작물 운용시스템을 복수의 단체가 운영하는 경우, 상기와 같이 각 단체는 독자적인 서비스 제공이 가능해진다. 또 마스터키와 서브그룹키와의 조합에 의해 이용할 수 있는 키의 수를 늘릴 수 있다는 효과가 있다.

여기에서, 상기 저작물 전송단계에서, 상기 기록매체장치와 상기 액세스장치가 모두 정당성을 갖는다고 인증된 경우에, 상기 액세스장치는, 상기 디지털 저작물을 분할하여 1이상의 데이터블록을 생성하고, 생성한 상기 데이터블록마다 데이터블록키를 생성하고, 상기 고유키와 상기 데이터블록에 대응하는 상기 데이터블록키를 이용하여 상기 데이터블록을 암호화하여 암호화 데이터블록을 생성하며, 생성한 암호화 데이터블록을 상기 기록매체장치로 전송하며, 혹은 상기 기록매체장치로부터 상기 암호화된 디지털 저작물을 구성하는 1이상의 암호화 데이터블록을 수신하고, 수신한 상기 암호화 데이터블록마다 데이터블록키를 생성하고, 상기 고유키와 상기 암호화 데이터블록에 대응하는 상기 데이터블록키를 이용하여 수신한 상기 암호화 데이터블록을 복호하며 데이터블록을 생성하며, 여기에서 상기 데이터블록은 논리적 단위길이 혹은 물리적 단위길이를 갖고, 상기 암호화 데이터블록은 논리적 단위길이 혹은 물리적 단위길이를 갖는 것으로 해도 된다.

이 구성에 의하면 저작물을 형성하는 데이터블록마다 다른 데이터블록키를 생성하고, 생성된 다른 데이터블록키로 데이터블록단위의 저작물을 암호화하기 때문에 데이터블록이 도청되기 어렵게 되어 데이터블록

의 안전성이 향상된다는 효과가 있다.

여기에서, 상기 저작물 전송단계에서, 상기 기록매체장치와 상기 액세스장치가 모두 정당성을 갖는다고 인증된 경우에, 상기 액세스장치는, 상기 디지털 저작물을 구성하는 파일마다 파일키를 생성하고, 상기 고유키와 상기 파일키를 이용하여 상기 파일을 암호화하여 암호화파일을 생성하며, 생성한 암호화파일과 파일키에 관한 정보를 상기 기록매체장치로 전송하며, 혹은 상기 기록매체장치로부터 상기 암호화된 디지털 저작물을 구성하는 파일과 파일키에 관한 정보를 수신하고, 수신한 파일마다 상기 고유키와 상기 파일키에 관한 정보를 이용하여 수신한 상기 파일을 복호함으로써 디지털 저작물을 재생하는 것으로 해도 된다.

이 구성에 의하면, 저작물을 형성하는 파일마다 다른 파일키를 생성하고, 생성된 다른 파일키로 파일단위의 저작물을 암호화하므로 파일이 도청되기 어렵게 되어 파일의 안전성이 향상된다는 효과가 있다.

여기에서, 상기 저작물 전송단계에서, 상기 기록매체장치와 상기 액세스장치가 모두 정당성을 갖는다고 인증된 경우에, 상기 액세스장치는, 조작자로부터 사용자키의 입력을 접수하고, 상기 입력을 접수한 사용자키와, 기억매체로부터 비밀전송된 고유키를 기초로 하여 변형키를 생성하고, 상기 변형키를 이용하여 상기 디지털 저작물을 암호화하여 상기 기록매체장치로 전송하며, 혹은 상기 기록매체장치로부터 상기 암호화된 디지털 저작물을 수신하고, 상기 변형키를 이용하여, 수신한 암호화된 디지털 저작물을 복호하여 디지털 저작물을 생성하는 것으로 해도 된다.

이 구성에 의하면, 사용자는 자신이 설정한 사용자키를 이용하여 저작물을 암호화하고, 암호화한 저작물을 상기 사용자키를 이용하여 복호할 수 있으므로 사용자 자신의 저작물이 타인에게 해독되지 않고, 보호할 수 있다는 효과가 있다.

여기에서, 암호화 고유키 작성장치가 추가로 포함되고, 디지털 저작물 보호시스템은, 상기 암호화 고유키 작성장치는 상기 기록매체장치가 소유하는 고유키에 암호를 실시하여 암호화 고유키를 생성하고, 상기 기록매체장치는 상기 생성된 암호화 고유키를 기억하는 암호화 고유키 설정단계를 가지며, 상기 인증단계에서, 상기 기록매체장치는 기억하고 있는 암호화 고유키를 상기 액세스장치에 전송하고, 상기 액세스장치는 취득한 상기 암호화 고유키를 복호하여 고유키를 생성하며, 생성한 상기 고유키를 이용하여 상기 기록매체장치의 정당성을 인증하는 것으로 해도 된다.

이 구성에 의하면 기록매체장치는 변환부를 갖지 않으므로 회로규모를 작게 할 수 있다는 효과를 갖는다.

상술한 목적과 본 발명의 특징 및 이점은 첨부도면과 관련한 다음의 상세한 설명을 통해 보다 분명해질 것이다.

이하 본 발명의 실시예에 대하여 도면을 참조하여 설명하기로 한다.

본 발명에 관한 일실시예로서의 디지털 저작물 보호시스템(100)에 대하여 설명하기로 한다.

1. 디지털 저작물 보호시스템(100)의 구성

디지털 저작물 보호시스템(100)은 도 1의 블록도에 도시된 바와 같이, 메모리카드(200), 메모리카드 기입기(300), 메모리카드 판독기(400)로 구성된다.

메모리카드(200)는 도 2에 도시된 바와 같이 메모리카드 삽입구(301)로부터 삽입되고, 메모리카드 기입기(300)에 장착된다. 또 메모리카드 기입기(300)는 메모리카드 기입기 삽입구(501)로부터 삽입되고, 퍼스널 컴퓨터(500)에 장착된다. 퍼스널 컴퓨터(500)는 통신회선(10)을 경유하여 인터넷으로 대표되는 네트워크에 접속되어 있고, 메모리카드 기입기(300)는 퍼스널 컴퓨터(500)를 개재하고 외부와 접속되어 있다.

퍼스널 컴퓨터(500)는 디스플레이(503), 키보드(504), 스피커(502), 도시하지 않는 프로세서, RAM, ROM, 하드디스크장치를 구비하고 있다.

메모리카드(200)는 메모리카드 판독기(400)에 장착된다. 메모리카드(200)는 도 3에 도시된 바와 같이 메모리카드 삽입구(403)로부터 삽입되고, 메모리카드 판독기(400)의 하나의 실시예로서의 헤드폰 스테레오(401)에 장착된다. 헤드폰 스테레오(401)는 상면에 조작버튼(404a, 404b, 404c, 404d)이 배치되고, 측면에 메모리카드 삽입구(403)를 갖고, 다른 측면에 헤드폰(402)이 접속되어 있다.

이용자는 메모리카드(200)를 메모리카드 기입기(300)를 통해 퍼스널컴퓨터 (500)에 장착하고, 인터넷을 경유하여 외부로부터 음악 등의 디지털 저작물을 인출하고, 인출된 디지털 저작물을 메모리카드(200)에 기입한다. 다음으로 이용자는, 디지털 저작물이 기록되어 있는 메모리카드(200)를 헤드폰 스테레오(401)에 장착하고, 메모리카드(200)에 기록되어 있는 디지털 저작물을 헤드폰 스테레오(401)에 의해 재생하고 즐긴다.

1. 1 메모리카드(200)의 구성

메모리카드(200)는 도 4에 도시된 바와 같이 마스터키 기억부(210), 미디어고유키 기억부(220), 변환부(230), 미디어고유키 정보기억부(240), 장치키 기억부 (221), 역변환부(222), 장치키 정보기억부(223), 상호인증부(250), 암호화 저작물 기억부(260), 통신부(270), 제어부(280)로 구성된다.

메모리카드(200)가 메모리카드 기입기(300)에 장착되면 통신부(270)는 메모리카드 기입기(300)의 후술하는 통신부(340)와 접속된다.

메모리카드(200)가 메모리카드 판독기(400)에 장착되면 통신부(270)는 메모리카드 판독기(400)의 후술하는 통신부(440)와 접속된다.

1. 1. 1 마스터키 기억부(210)

마스터키 기억부(210)는 구체적으로는 반도체 메모리 등으로 구성되고, 미리 하나의 마스터키 Mk를 기억하고 있다. 마스터키 Mk는 56비트의 비트열로 이루어진다. 마스터키는 디지털 저작물 운용시스템마다 다

르다. 또 특정한 디지털 저작물 운용시스템을 위해 이용되는 모든 메모리카드의 마스터키 기억부는, 예를 들면 이들의 메모리카드가 다른 메이커에 의해 제조된 것이더라도 같은 마스터키를 기억하고 있다.

여기에서 디지털 저작물 운용시스템이란 예를 들면, A사, B사, C사의 3사가 공동으로 운영하여, 음악을 배포하는 음악배포 시스템이고, 또 X사, Y사, Z사가 공동으로 운영하는 영화임대제도가 있다.

1. 1. 2 미디어고유키 기억부(220)

미디어고유키 기억부(220)는 구체적으로는 반도체 메모리 등으로 구성되고, 미리 하나의 고유키 Ki를 기억하고 있다. 고유키 Ki는 56비트의 비트열로 이루어진다. 고유키는 제조되는 메모리카드마다 다르다. 고유키는 제조되는 메모리카드마다 다른 메모리카드의 제조번호와, 메모리카드가 제조될 때마다 생성되는 난수에 소정의 연산을 실시하여, 예를 들면 가산을 실시하여 산출된다.

1. 1. 3 변환부(230)

변환부(230)는 구체적으로는 프로세서, 프로그램을 기억하고 있는 ROM(Read Only Memory), 작업용의 RAM(Random Access Memory) 등으로 구성되고, 미디어고유키 기억부(220)에 기억되어 있는 고유키 Ki를 판독하고, 마스터키 기억부(210)에 기억되어 있는 마스터키 Mk를 판독한다.

변환부(230)는 DES(데이터 암호화규격, Data Encryption Standard)에 의해 규격되어 있는 암호알고리즘 E1을 미리 기억하고 있다.

여기에서 DES에 의해 규격되어 있는 암호알고리즘 E1은 암호키는 56비트이고, 평문 및 암호문의 길이는 64비트이다. 또, 이 실시예에 있어서, 암호알고리즘 및 복호알고리즘은 특별히 설명하지 않는 한, DES에 의해 규격되어 있는 알고리즘이고, 암호키 및 복호키는 56비트이고, 평문 및 암호문의 길이는 64비트이다.

변환부(230)는 판독한 고유키 Ki에 암호알고리즘 E1을 실시하여 암호화 고유키 Ji를 생성한다. 이 때, 상기 판독한 마스터키 Mk를 암호알고리즘 E1의 키로 한다. 생성된 암호화 고유키 Ji는 다음의 수학식 1에 도시된 바와 같이 표현한다.

$$Ji = E1\ (Mk,\ Ki)$$

또 이 명세서에 있어서, 키 K를 이용하여 평문 M에 대하여 암호알고리즘 E를 실시하고, 암호문 C을 생성할 때 다음의 수학식 2에 나타낸 바와 같이 표현하는 것으로 한다.

$$C = E\ (K,\ M)$$

또 키 K를 이용하여 상기 생성된 암호문 C에 대하여 복호알고리즘 D를 실시하고, 상기 평문 M을 생성할 때 다음의 수학식 3에 나타낸 바와 같이 표현하는 것으로 한다.

$$M = D\ (K,\ C)$$

이와 같이 키 K를 이용하여 평문 M에 대하여 암호알고리즘 E를 실시하여 암호문 C을 생성하고, 생성된 암호문 C에 대하여 복호알고리즘 D를 실시하고, 상기 평문 M과 동일한 평문이 생성될 때 암호알고리즘 E와 복호알고리즘 D의 관계를 다음의 수학식 4에 나타낸 바와 같이 표현하는 것으로 한다.

$$M = decrypt\ (D)$$

변환부(230)는 생성된 암호화 고유키 Ji를 미디어고유키 정보기억부(240)로 출력한다.

1. 1. 4 미디어고유키 정보기억부(240)

미디어고유키 정보기억부(240)는 구체적으로는 반도체 메모리 등으로 구성되고, 변환부(230)로부터 암호화 고유키 Ji를 수취하고, 수취한 암호화 고유키 Ji를 기억한다.

1. 1. 5 상호인증부(250)

상호인증부(250)는 난수발생부(251), 암호부(252), 복호부(253), 상호인증 제어부(254)로 구성된다. 이들의 상호인증부(250)를 구성하는 각 구성요소는 구체적으로는 프로세서, 프로그램을 기억하고 있는 ROM, 작업용 RAM 등으로 구성된다.

(1) 난수발생부(251)

난수발생부(251)는 난수 R_a를 생성한다. 난수 R_a는 64비트의 비트열로 이루어진다. 난수발생부(251)는 생성한 난수 R_a를 통신부(270)와 상호인증 제어부(254)로 출력한다.

(2) 암호부(252)

암호부(252)는 통신부(270)로부터 난수 R_b을 수취한다.

암호부(252)는 미디어고유키 기억부(220)로부터 고유키 Ki를 판독한다.

암호부(252)는 DES에 의해 규격되어 있는 암호알고리즘 E_2를 미리 기억하고 있다.

암호부(252)는 수취한 난수 R_1에 암호알고리즘 E_2를 실시하고 암호화난수 S_1 을 생성한다. 이 때 상기 판독한 고유키 KI를 암호알고리즘 E_2의 키로 한다. 생성된 암호화난수 S_1은 다음의 수학식 5에 나타낸 바와 같이 표현할 수 있다.

$$S_1 = E_2 (KI, R_1)$$

암호부(252)는 생성한 암호화난수 S_1을 통신부(270)로 출력한다.

(3)복호부(253)

복호부(253)는 통신부(270)로부터 암호화난수 S_2를 수취하고, 장치키 기억부 (221)로부터 장치키 AJ를 판독한다.

복호부(253)는 DES에 의해 규격되어 있는 복호알고리즘 D_2를 미리 기억하고 있다.

복호부(253)는 수취한 암호화난수 S_2에 복호알고리즘 D_2를 실시하여 난수 R_2를 생성한다. 이 때 상기 판독한 장치키 AJ를 복호알고리즘 D_2의 키로 한다. 생성된 난수 R_2는 다음의 수학식 6에 나타낸 바와 같이 표현할 수 있다.

$$R_2 = D_2 (AJ, S_2)$$

$$D_2 (AJ, E_2 (AJ, R_2))$$

복호부(253)는 생성한 난수 R_2를 상호인증 제어부(254)로 출력한다.

(4) 상호인증 제어부(254)

상호인증 제어부(254)는 복호부(253)로부터 난수 R_2를 수취한다. 또 상호인증 제어부(254)는 난수발생부 (251)로부터 난수 R_1를 수취한다.

상호인증 제어부(254)는 복호부(253)로부터 수취한 난수 R_2와, 난수발생부 (251)로부터 수취한 난수 R_1를 비교하여, 난수 R_2와 난수 R_1가 일치하면 메모리카드 (200)가 장착된 메모리카드 기입기(300) 또는 메모리카드 판독기(400)가 정당한 장치라고 인증하고, 난수 R_2와 난수 R_1가 일치하지 않으면 메모리카드(200)가 장착된 메모리카드 기입기(300)또는 메모리카드 판독기(400)가 부정한 장치로 간주한다.

상호인증 제어부(254)는 메모리카드 기입기(300) 또는 메모리카드 판독기 (400)가 정당한 장치인지 부정한 장치인지를 나타내는 인증신호를 제어부(280)에 출력한다.

1. 1. 6 암호화저작물 기억부(260)

암호화저작물 기억부(260)는 기억매체로서 반도체 메모리를 갖는다.

암호화저작물 기억부(260)는 통신부(270)로부터 암호화 부분저작물 F_i(i=1, 2, 3, ···)를 수취하고, 수취한 암호화 부분저작물 F_i(i=1, 2, 3, ···)를 기억한다.

1. 1. 7 통신부(270)

통신부(270)는 미디어고유키 정보기억부(240)로부터 암호화 고유키 JI 를 판독하고, 판독한 암호화 고유키 JI를 메모리카드 기입기(300)의 통신부(340) 또는 메모리카드 판독기(400)의 통신부(440)로 출력한다.

통신부(270)는 메모리카드 기입기(300)의 통신부(340)로부터 또는 메모리카드 판독기(400)의 통신부(440)로부터 난수 R_1을 수취하고, 수취한 난수 R_1을 상호인증부(250)의 암호부(252)로 출력한다.

통신부(270)는 암호부(252)로부터 암호화난수 S_1을 수취하고, 수취한 암호화난수 S_1을 메모리카드 기입기(300)의 통신부(340) 또는 메모리카드 판독기(400)의 통신부(440)로 출력한다.

통신부(270)는 메모리카드 기입기(300)의 통신부(340) 또는 메모리카드 판독기(400)의 통신부(440)로부터 암호화장치키 B_i를 수취하고, 수취한 암호화장치키 B_i를 장치키 정보기억부(223)로 출력한다.

통신부(270)는 난수발생부(251)로부터 난수 R_1를 수취하고, 수취한 난수 R_1를 메모리카드 기입기(300)의 통신부(340) 또는 메모리카드 판독기(400)의 통신부 (440)로 출력한다.

통신부(270)는 메모리카드 기입기(300)의 통신부(340) 또는 메모리카드 판독기(400)의 통신부(440)로부터 암호화난수 S_2를 수취하고, 수취한 암호화난수 S_2를 상호인증부(250)의 복호부(253)로 출력한다.

통신부(270)는 제어부(280)로부터 통신중지신호를 수취하면 메모리카드 기입기(300)의 통신부(340), 또는 메모리카드 판독기(400)의 통신부(440)와의 통신을 중지한다.

통신부(270)는 메모리카드 기입기(300)의 통신부(340)로부터 암호화 부분저작물 F_i(i=1, 2, 3, ···)를

수취하고, 수취한 암호화 부분저작물 F_i(i=1, 2, 3, ...)를 암호화저작물 기억부(260)로 출력한다.

통신부(270)는, 암호화저작물 기억부(260)로부터 암호화저작물을 판독하고, 판독한 암호화저작물을 메모리카드 판독기(400)의 통신부(440)로 출력한다.

1. 1. 8 장치키 정보기억부(223)

장치키 정보기억부(223)는 구체적으로는, 반도체 메모리 등으로 구성되고, 통신부(270)로부터 암호화장치키 B_i를 수취하고, 수취한 암호화장치키 B_i를 기억한다.

1. 1. 9 역변환부(222)

역변환부(222)는 구체적으로는 프로세서, 프로그램을 기억하고 있는 ROM, 작업용 RAM 등으로 구성되며, 장치키 정보기억부(223)로부터 암호화장치키 B_i를 판독하고, 마스터키 기억부(210)에 기억되어 있는 마스터키 Mk를 판독한다.

역변환부(222)는 DES에 의해 규격되어 있는 복호알고리즘 D_k을 미리 기억하고 있다.

역변환부(222)는 판독한 암호화장치키 B_i에 복호알고리즘 D_k을 실시하여 장치키 A_i를 생성한다. 이 때 상기 판독한 마스터키 Mk를 복호알고리즘 D_k의 키로 한다. 생성된 장치키 A_i는 다음의 수학식 7에 나타낸 바와 같이 표현할 수 있다.

$$A_i = D_k(Mk, B_i) = D_k(Mk, E_k(Mk, A_i))$$

역변환부(222)는 생성한 장치키 A_i를 장치키 기억부(221)로 출력한다.

1. 1. 10 장치키 기억부(221)

장치키 기억부(221)는 구체적으로는 반도체 메모리 등으로 구성되고, 역변환부(222)로부터 출력된 장치키 A_i를 기억한다.

1. 1. 11 제어부(280)

제어부(280)는 구체적으로는 프로세서, 프로그램을 기억하고 있는 ROM, 작업용 RAM 등으로 구성되며, 상호인증 제어부(254)로부터 메모리카드(200)가 장착된 메모리카드 기입기(300) 또는 메모리카드 판독기(400)가 정당한 장치인지 부정한 장치인지를 나타내는 인증신호를 수취한다.

제어부(280)는 수취한 인증신호가 부정한 장치라는 것을 나타내는 경우에는 메모리카드 기입기(300) 또는 메모리카드 판독기(400)와의 통신을 중지하는 통신중지신호를 통신부(270)로 출력한다.

1. 2 메모리카드 기입기(300)의 구성

메모리카드 기입기(300)는 도 5에 도시된 바와 같이 장치키 기억부(310), 변환부(311), 장치키 정보기억부(312), 마스터키 기억부(313), 미디어고유키 정보기억부(320), 역변환부(321), 미디어고유키 기억부(323), 상호인증부(330), 통신부 (340), 제어부(350), 암호부(360), 저작물 기억부(370), 저작물 취득부(380)로 구성된다.

저작물 취득부(380)는 통신회선(10)을 경유하여 외부와 접속되어 있다.

1. 2. 1 장치키 기억부(310)

장치키 기억부(310)는 구체적으로는 반도체 메모리 등으로 구성되고, 미리 하나의 장치키 A_i를 기억하고 있다. 장치키 A_i는 56비트의 비트열로 이루어진다. 장치키는 제조되는 메모리카드 기입기마다 다르다. 장치키는 제조되는 메모리카드 기입기마다 다른 메모리카드 기입기의 제조번호와, 메모리카드 기입기가 제조될 때마다 생성되는 난수와, 소정의 연산을 실시하고, 예를 들면 가산을 실시하여 산출된다.

1. 2. 2 변환부(311)

변환부(311)는 구체적으로는 프로세서, 프로그램을 기억하고 있는 ROM, 작업용 RAM 등으로 구성되며, 장치키 기억부(310)에 기억되어 있는 장치키 A_i를 판독하고, 마스터키 기억부(313)에 기억되어 있는 마스터키 Mk를 판독한다.

변환부(311)는 DES에 의해 규격되어 있는 암호알고리즘 E_k을 미리 기억하고 있다.

메모리카드(200)의 역변환부(222)에 기억되어 있는 복호알고리즘 D_k과 암호알고리즘 E_k 사이에는 다음의 수학식 8에 나타낸 바와 같은 관계가 있다.

$$E_k = D_k^{-1}$$

변환부(311)는 판독한 장치키 A_i에 암호알고리즘 E_k을 실시하여 암호화장치키 B_i를 생성한다. 이 때 상기 판독한 마스터키 Mk를 암호알고리즘 E_k의 키로 한다. 생성된 암호화장치키 B_i는 다음의 수학식 9에 나타낸

바와 같이 표현할 수 있다.

$$B_i = E_3 (Mk, A_i)$$

변환부(311)는 생성한 암호화장치키 B_i를 장치키 정보기억부(312)로 출력한다.

1. 2. 3 장치키 정보기억부(312)

장치키 정보기억부(312)는 구체적으로는 반도체 메모리 등으로 구성되며, 변환부(311)로부터 암호화장치키 B_i를 수취하고, 수취한 암호화장치키 B_i를 기억한다.

1. 2. 4 마스터키 기억부(313)

마스터키 기억부(313)는 구체적으로는 반도체 메모리 등으로 구성되며, 미리 하나의 마스터키 Mk를 기억하고 있다. 마스터키 Mk는 메모리카드(200)의 마스터키 기억부(210)가 기억하고 있는 마스터키와 동일하다.

1. 2. 5 미디어고유키 정보기억부(320)

미디어고유키 정보기억부(320)는 구체적으로는 반도체 메모리 등으로 구성되며, 통신부(340)로부터 암호화 고유키 Ji를 수취하고, 수취한 암호화 고유키 Ji를 기억한다.

1. 2. 6 역변환부(321)

역변환부(321)는 구체적으로는 프로세서, 프로그램을 기억하고 있는 ROM, 작업용 RAM 등으로 구성되며, 미디어고유키 정보기억부(320)에 기억되어 있는 암호화 고유키 Ji를 판독하고, 마스터키 기억부(313)에 기억되어 있는 마스터키 Mk를 판독한다.

역변환부(321)는 DES에 의해 규격되어 있는 복호알고리즘 D_i를 미리 기억하고 있다.

메모리카드(200)의 변환부(230)에 기억되어 있는 암호알고리즘 E_i과 복호알고리즘 D_i 사이에는, 다음의 수학식 10에 나타내는 관계가 있다.

$$E_i = crypt(D_i)$$

역변환부(321)는 판독한 암호화 고유키 Ji에 복호알고리즘 D_i을 실시하여 고유키 K'i를 생성한다. 이 때 상기 판독한 마스터키 Mk를 복호알고리즘 D_i의 키로 한다. 생성된 고유키 K'i는 다음의 수학식 11에 나타낸 바와 같이 표현할 수 있다.

$$K'i = D_i (Mk, Ji)$$
$$= D_i (Mk, E_i (Mk, Ki))$$

역변환부(321)는 생성한 고유키 K'i를 미디어고유키 기억부(323)로 출력한다.

1. 2. 7 미디어고유키 기억부(323)

미디어고유키 기억부(323)는 구체적으로는 반도체 메모리 등으로 구성되며, 역변환부(321)로부터 고유키 K'i를 수취하고, 수취한 고유키 K'i를 기억한다.

1. 2. 8 상호인증부(330)

상호인증부(330)는 난수발생부(331), 암호부(332), 복호부(333), 상호인증 제어부(334)로 구성된다. 상호인증부(330)를 구성하는 각 구성요소는 구체적으로는 프로세서, 프로그램을 기억하고 있는 ROM, 작업용 RAM 등으로 구성된다.

(1) 난수발생부(331)

난수발생부(331)는 난수 R_i을 생성한다. 난수 R_i은 64비트의 비트열로 이루어진다. 난수발생부(331)는 생성한 난수 R_i을 통신부(340)로 출력한다. 또 난수발생부 (331)는 생성한 난수 R_i을 상호인증 제어부(334)로 출력한다.

(2) 암호부(332)

암호부(332)는 통신부(340)로부터 난수 R_2를 수취하고, 장치키 기억부(310)로부터 장치키 A_i를 판독한다.

암호부(332)는 DES에 의해 규격되어 있는 암호알고리즘 E_3를 미리 기억하고 있다.

암호부(332)는 수취한 난수 R_2에 암호알고리즘 E_3를 실시하여 암호화난수 S_2를 생성한다. 이 때 상기 판독한 장치키 A_i를 암호알고리즘 E_3의 키로 한다. 생성된 암호화난수 S_2는 다음의 수학식 12에 나타낸 바와 같이 표현할 수 있다.

$$S_i = E_i(A_i, R_i)$$

암호부(332)는 생성한 암호화난수 S_i를 통신부(340)로 출력한다.

(3)복호부(333)

복호부(333)는 통신부(340)로부터 암호화난수 S_i을 수취한다.

복호부(333)는 미디어고유키 기억부(323)로부터 고유키 $K'i$를 판독한다.

복호부(333)는 OES에 의해 규격되어 있는 복호알고리즘 D_i를 미리 기억하고 있다.

메모리카드(200)의 상호인증부(330)의 암호부(252)에 기억되어 있는 암호알고리즘 E_i와 복호알고리즘 D_i 사이에는 다음의 수학식 13에 나타내는 관계가 있다.

$$E_i = c\,r\,p\,t\,(D_i)$$

복호부(333)는 수취한 암호화난수 S_i에 복호알고리즘 D_i를 실시하여 난수 R'_i을 생성한다. 이 때 상기 판독한 고유키 $K'i$를 복호알고리즘 D_i의 키로 한다. 생성된 난수 R'_i은 다음의 수학식 14에 나타낸 바와 같이 표현할 수 있다.

$$R'_i = D_i(K'i, S_i) = D_i(K'i, E_i(Ki, R_i))$$

복호부(333)는 생성된 난수 R'_i을 상호인증 제어부(334)로 출력한다.

(4) 상호인증 제어부(334)

상호인증 제어부(334)는 복호부(333)로부터 난수 R'_i을 수취한다. 또 상호인증 제어부(334)는 난수발생부(331)로부터 난수 R_i을 수취한다.

상호인증 제어부(334)는 복호부(333)로부터 수취한 난수 R'_i과 난수발생부 (331)로부터 수취한 난수 R_i을 비교하여, 난수 R'_i과 난수 R_i이 일치하면 메모리카드 기입기(300)에 장착된 메모리카드(200)가 정당한 장치라고 인증하고, 난수 R'_i과 난수 R_i이 일치하지 않으면 메모리카드 기입기(300)에 장착된 메모리카드(200)가 부정한 장치라고 간주한다.

상호인증 제어부(334)는 메모리카드 기입기(300)에 장착된 메모리카드(200)가 정당한 장치인지 부정한 장치인지를 나타내는 인증신호를 제어부(350)로 출력한다.

1, 2, 9 통신부(340)

통신부(340)는 메모리카드(200)의 통신부(270)로부터 암호화 고유키 Ji를 수취하고, 수취한 암호화 고유키 Ji를 미디어고유키 정보기억부(320)로 출력한다.

통신부(340)는 난수발생부(331)로부터 난수 R_i을 수취하고, 수취한 난수 R_i을 메모리카드(200)의 통신부(270)로 출력한다.

통신부(340)는 메모리카드(200)의 통신부(270)로부터 암호화난수 S_i을 수취하고, 수취한 암호화난수 S_i을 상호인증부(330)의 복호부(333)로 출력한다.

통신부(340)는 장치키 정보기억부(312)로부터 암호화장치키 B_i를 판독하고, 판독한 암호화장치키 B_i를 메모리카드(200)의 통신부(270)로 출력한다.

통신부(340)는 메모리카드(200)의 통신부(270)로부터 난수 R_i를 수취하고, 수취한 난수 R_i를 상호인증부(330)의 암호부(332)로 출력한다.

통신부(340)는 암호부(332)로부터 암호화난수 S_i를 수취하고, 수취한 암호화난수 S_i를 메모리카드(200)의 통신부(270)로 출력한다.

통신부(340)는 제어부(350)로부터 통신중지신호를 수취하면 메모리카드(200)의 통신부(270)의 통신을 중지한다.

통신부(340)는 암호부(360)로부터 암호화부분저작물 $F_i(i=1, 2, 3, \cdots)$를 수취하고, 수취한 암호화 부분저작물 $F_i(i=1, 2, 3, \cdots)$를 메모리카드(200)의 통신부(270)로 출력한다.

1, 2, 10 제어부(350)

제어부(350)는 구체적으로는 프로세서, 프로그램을 기억하고 있는 ROM, 작업용 RAM 등으로 구성되고, 상

호인증 제어부(334)로부터 메모리카드 기입기(300)에 장착된 메모리카드(200)가 정당한 장치인지 부정한 장치인지를 나타내는 인증신호를 수취한다.

제어부(350)는, 수취한 인증신호가 부정한 장치인 것을 나타내는 경우에는 메모리카드(200)와의 통신을 중지하는 통신중지신호를 통신부(340)로 출력한다.

제어부(350)는 수취한 인증신호가 정당한 장치인 것을 나타내는 경우에는 저작물 취득부(380)에 대하여 외부로부터의 저작물취득을 지시하는 저작물 취득신호를 출력한다.

1. 2. 11 저작물 취득부(380)

저작물 취득부(380)는 제어부(350)로부터 저작물 취득신호를 수취한다.

저작물 취득부(380)는 제어부(350)로부터 저작물 취득신호를 수취하면 통신회선(10)을 경유하여 외부로부터 음악의 저작물을 취득하고, 취득한 저작물을 저작물 기억부(370)로 출력한다.

또 여기에서 저작물은 음악이라고 하고 있지만, 음악에 한정되지 않는 것은 물론이다. 그 밖의 문서, 화상, 영화 등도 저작물에 포함된다.

1. 2. 12 저작물 기억부(370)

저작물 기억부(370)는 구체적으로는 반도체 메모리 등으로 구성되며, 저작물 취득부(380)로부터 저작물을 수취하고, 수취한 저작물을 기억한다.

1.2 13 암호부(360)

암호부(360)는 구체적으로는 프로세서, 프로그램을 기억하고 있는 ROM, 작업용 RAM 등으로 구성되며, 저작물 기억부(370)로부터 저작물을 판독하고, 미디어고유키 기억부(323)로부터 고유키 K_i를 판독한다.

암호부(360)는 DES에 의해 규격되어 있는 암호알고리즘 E_2를 미리 기억하고 있다.

암호부(360)는 판독한 저작물을 복수의 64비트의 비트열로 이루어지는 부분저작물 C_i(i=1, 2, 3, ···)로 분할하고, 각 부분저작물 C_i(i=1, 2, 3, ···) 에 암호알고리즘 E_2를 실시하여 복수의 암호화 부분저작물 F_i(i=1, 2, 3, ···) 를 생성한다. 이 때 상기 판독한 고유키 K_i를 암호알고리즘 E_2의 키로 한다. 생성된 암호화 부분저작물 F_i(i=1, 2, 3, ···)는 다음의 수학식 15에 나타낸 바와 같이 표현할 수 있다.

$$F_i = E_2(K_i, C_i) \quad (i = 1, 2, 3, \cdots) \qquad \text{수학식 15}$$

암호부(360)는 생성한 암호화 부분저작물 F_i(i=1, 2, 3, ···)를 통신부 (340)로 출력한다.

1. 3 메모리카드 판독기(400)의 구성

메모리카드 판독기(400)는 도 6에 도시된 바와 같이 장치키 기억부(410), 변환부(411), 장치키 정보기억부(412), 마스터키 기억부(413), 미디어고유키 정보기억부(420), 역변환부(421), 미디어고유키 기억부(423), 상호인증부(430), 통신부 (440), 제어부(450), 복호부(460), 저작물 기억부(470), 재생부(480), 조작부(490)로 구성된다.

장치키 기억부(410), 변환부(411), 장치키 정보기억부(412), 마스터키 기억부(413), 미디어고유키 정보기억부(420), 역변환부(421), 미디어고유키 기억부 (423), 상호인증부(430), 통신부(440), 제어부(450)에 대해서는 각각 메모리카드 판독기(400)의 장치키 기억부(310), 변환부(311), 장치키 정보기억부(312), 마스터키 기억부(313), 미디어고유키 정보기억부(320), 역변환부(321), 미디어고유키 기억부(323), 상호인증부(330), 통신부(340), 제어부(350)와 동등하므로 동등부분의 설명은 생략하고, 다른 기능, 작용을 갖는 점을 중심으로 하여 설명한다.

1. 3. 1 제어부(450)

제어부(450)는 수취한 인증신호가 정당한 장치인 것을 나타내는 경우에는 복호부(460)에 대하여 통신부(440)로부터 출력되는 암호화저작물의 복호를 지시하는 복호지시를 출력한다.

1. 3. 2 복호부(460)

복호부(460)는 제어부(450)로부터 복호지시를 수취한다.

복호부(460)는 제어부(450)로부터 복호지시를 수취하면 통신부(440)로부터 암호화저작물을 수취하고, 미디어고유키 기억부(423)로부터 고유키 K_i를 판독한다.

복호부(460)는 DES에 의해 규격되어 있는 복호알고리즘 D_2를 미리 기억하고 있다.

복호부(460)는 수취한 암호화저작물을 복수의 64비트의 비트열로 이루어지는 부분암호화 저작물 G_i(i=1, 2, 3, ···)로 분할하고, 각 부분암호화 저작물 G_i (i=1, 2, 3, ···)에 복호알고리즘 D_2를 실시하여 복수의 부분저작물 H_i(i=1, 2, 3, ···)을 생성한다. 이 때 상기 판독한 고유키 K_i를 복호알고리즘 D_2의 키로 한다. 생성된 부분저작물 H_i(i=1, 2, 3, ···)는 수학식 16에 나타낸 바와 같이 표현할 수 있다.

$$H_i = D_{K'i}(G_i) \quad (i = 1, 2, 3, \cdots)$$

복호부(460)는 생성한 부분저작물 $H_i(i=1, 2, 3, \cdots)$를 저작물 기억부 (470)로 출력한다.

1. 3. 3 저작물 기억부(470)

저작물 기억부(470)는 복호부(460)로부터 부분저작물 $H_i(i=1, 2, 3, \cdots)$를 수취하고, 수취한 부분저작물 $H_i(i=1, 2, 3, \cdots)$를 기억한다.

1. 3. 4 조작부(490)

조작부(490)는 각종 사용자의 지시를 접수하는 복수의 조작버튼을 갖고 있다.

각종 사용자의 지시에 대응하는 조작버튼이 사용자에 의해 조작되면 조작된 조작버튼에 대응하는 지시를 재생부(480)에 출력한다.

1. 3. 5 재생부(480).

재생부(480)는 조작부(490)로부터 지시를 수취한다.

재생부(480)는 수취한 지시에 기초하여 저작물 기억부(470)에 기억되어 있는 음악의 저작물을 판독하고, 판독한 저작물을 재생한다.

2. 디지털 저작물 보호시스템(100)의 동작

디지털 저작물 보호시스템(100)의 동작에 대하여 설명한다.

2.1 메모리카드(200)가 메모리카드 기입기(300)에 장착된 경우의 개요동작

메모리카드(200)가 메모리카드 기입기(300)에 장착된 경우의 개요동작에 대하여 도 7에 도시된 흐름도를 이용하여 설명한다.

메모리카드(200)가 메모리카드 기입기(300)에 장착되면 메모리카드 기입기 (300)가 메모리카드(200)를 인증하고(단계 S110), 메모리카드 기입기(300)가 메모리카드(200)는 부정한 장치라고 인식한 경우에는(단계 S111), 메모리카드 기입기 (300)와 메모리카드(200) 사이에서 통신을 하지 않고, 처리를 종료한다.

메모리카드 기입기(300)가 메모리카드(200)는 정당한 장치라고 인식한 경우에는(단계 S111), 메모리카드(200)가 메모리카드 기입기(300)를 인증하고(단계 S112) , 메모리카드(200)가 메모리카드 기입기(300)는 부정한 장치라고 인식한 경우에는 (단계 S113), 메모리카드 기입기(300)와 메모리카드(200) 사이에서 통신을 하지 않고 처리를 종료한다.

메모리카드(200)가 메모리카드 기입기(300)는 정당한 장치라고 인식한 경우에는(단계 S113), 메모리카드 기입기(300)는 외부로부터 저작물을 취득하고, 취득한 저작물을 암호화하며, 암호화된 저작물을 메모리카드(200)로 출력하고(단계 S114), 메모리카드(200)는 암호화된 저작물을 기억한다(단계 S115).

2. 2 메모리카드(200)가 메모리카드 판독기(400)에 장착된 경우의 개요동작

메모리카드(200)가 메모리카드 판독기(400)에 장착된 경우의 개요동작에 대하여 도 8에 도시된 흐름도를 이용하여 설명한다.

메모리카드(200)가 메모리카드 판독기(400)에 장착되면 메모리카드 판독기 (400)가 메모리카드(200)를 인증하고(단계 S120), 메모리카드 판독기(400)가 메모리카드(200)는 부정한 장치라고 인식한 경우에는(단계 S121), 메모리카드 판독기 (400)와 메모리카드(200) 사이에서 통신을 하지 않고 처리를 종료한다.

메모리카드 판독기(400)가 메모리카드(200)는 정당한 장치라고 인식한 경우에는(단계 S121), 메모리카드(200)가 메모리카드 판독기(400)를 인증하고(단계 S122) , 메모리카드(200)가 메모리카드 판독기(400)는 부정한 장치라고 인식한 경우에는 (단계 S123), 메모리카드 판독기(400)와 메모리카드(200) 사이에서 통신을 하지 않고 처리를 종료한다.

메모리카드(200)가 메모리카드 판독기(400)는 정당한 장치라고 인식한 경우에는(단계 S123), 메모리카드(200)는 암호화된 저작물을 메모리카드 판독기(400)로 출력하고(단계 S124), 메모리카드 판독기(400)는 메모리카드(200)로부터 출력된 암호된 저작물을 복호하고(단계 S125), 메모리카드 판독기(400)는 복호된 저작물을 재생한다(단계 S126) .

2. 3 메모리카드(200)가 메모리카드 기입기(300)에 장착된 경우의 상세한 인증동작

메모리카드(200)가 메모리카드 기입기(300)에 장착된 경우의 상세한 인증동작에 대하여 도 9 및 도 10을 이용하여 설명한다.

변환부(230)는 마스터키 Mk를 암호알고리즘 E_1의 키로서, 고유키 Ki에 암호알고리즘 E_1을 실시하여 암호화 고유키 $E_1(Mk, Ki)$을 생성하고(단계 S130), 통신부 (270)는 암호화 고유키 $E_1(Mk, Ki)$을 통신부(340)를 경유하여 역변환부(321)로 출력하고(단계 S131), 역변환부(321)는 마스터키 Mk를 복호알고리즘 D_1의 키로서 암호화 고유키 $E_1(Mk, Ki)$에 복호알고리즘 D_1을 실시하여 고유키 $K_i=(Mk, E_1(Mk, Ki))$를 생성하고(단계 S132), 난수발생부(331)는 난수 R_i을 생성하고(단계 S133), 통신부 (340)는 생성된 난수 R_i을 통신부(270)를 경유하여 암호부(252)로 출력하고(단계 S134), 암호부(252)는 고유키 Ki를 암호알고리즘 E_2의 키로서 난수 R_i에 암호알고리즘 E_2를 실시하여 암호화난수 $E_2(Ki, R_i)$를 생성하고(단계 S135), 통신부(270)는 통신

부(340)를 경유하여 암호화난수 $E_2(Ki, R_1)$를 복호부(333)로 출력하고(단계 S136), 복호부(333)는 고유키 K$_i$를 복호알고리즘 D_2의 키로서 암호화난수 $E_2(Ki, R_1)$에 복호알고리즘 D_2를 실시하고, $D_2(K_i, E_2(Ki, R_1))$를 생성하고(단계 S137), 상호인증 제어부(334)는 난수 R_1과 $D_2(K_i, E_2(Ki, R_1))$를 비교하고, 일치하고 있으면 메모리카드(200)는 정당한 장치라고 인식하고, 일치하지 않으면 메모리카드(200)는 부정한 장치라고 인식한다(단계 S138).

변환부(311)는 마스터키 Mk를 암호알고리즘 E_4의 키로서 장치키 A_i에 암호알고리즘 E_4를 실시하고 암호화장치키 $E_4(Mk, A_i)$을 생성하고(단계 S139), 통신부 (340)는 암호화장치키 $E_4(Mk, A_i)$을 통신부(270)를 경유하여 역변환부(222)로 출력하고(단계 S140), 역변환부(222)는 마스터키 Mk를 복호알고리즘 D_4의 키로 하여 암호화장치키 $E_4(Mk, A_i)$에 복호알고리즘 D_4를 실시하여 장치키 $A' = D_4(Mk, E_4(Mk, A_i))$을 생성하고(단계 S141), 난수발생부(251)는 난수 R_2를 생성하고(단계 S142), 통신부(270)는 생성된 난수 R_2를 통신부(340)를 경유하여 암호부(332)로 출력하고(단계 S143), 암호부(332)는 장치키 A_i를 암호알고리즘 E_2의 키로 하여 난수 R_2에 암호알고리즘 E_2를 실시하여 암호화난수 $E_2(A_i, R_2)$를 생성하고(단계 S144), 통신부(340)는 통신부(270)를 경유하여 암호화난수 $E_2(A_i, R_2)$를 복호부(253)로 출력하고(단계 S145), 복호부(253)는 장치키 A_i를 복호알고리즘 D_2의 키로 하여 암호화난수 $E_2(A_i, R_2)$에 복호알고리즘 D_2를 실시하여 $D_2(A_i, E_2(A_i, R_2))$를 생성하고(단계 S146), 상호인증 제어부(254)는 난수 R_2와 $D_2(A_i, E_2(A_i, R_2))$를 비교하여 일치하면 메모리카드 기입기(300)는 정당한 장치라고 인식하고, 일치하지 않으면 메모리카드 기입기 (300)는 부정한 장치라고 인식한다(단계 S147).

2. 4 정리

이상 설명한 바와 같이 메모리카드를 일례로 하는 암호화된 디지털 저작물을 기억하는 영역을 갖는 기록매체장치와, 메모리카드 기입기 또는 메모리카드 판독기를 일례로 하는 상기 영역으로부터 정보를 판독 또는 상기 영역으로 정보를 기입하는 액세스장치는 각 장치가 접속된 경우에 서로 상대의 장치가 정당한 장치인지 부정한 장치인지를 인증하여 서로 정당한 장치라고 인증된 경우에만 기록매체장치로부터 액세스장치로 저작물을 전송하고, 또는 액세스장치로부터 기록매체장치로 저작물을 전송한다. 이 구성에 의해 정당한 장치로부터 부정한 장치로 저작물을 전송하는 것을 방지할 수 있으므로 정당하게 취득된 저작물이 부정하게 이용되는 것을 방지할 수 있는 것과 아울러, 또 부정한 장치로부터 정당한 장치로 저작물을 전송하는 것을 방지할 수 있으므로 부정하게 취득된 저작물의 이용을 방지할 수 있다. 이와 같이 정당한 액세스장치가 행한 인증순서를 모방하는 부정한 기록장치의 재실행 공격에 견딜 수 있는 강고한 인증처리를 실현할 수 있고, 부정한 장치가 정당한 장치를 속여 저작물을 부정하게 판독하거나 또는 저작물을 부정하게 기입하는 것을 방지할 수 있다.

또 기록매체장치는 소유하는 고유키를 마스터키를 이용하여 액세스장치에 비밀전송하고, 액세스장치는 난수로서 생성한 인증정보를 기록매체장치에 전송하고 기록매체장치는 상기 고유키를 이용하여 상기 인증정보에 암호를 실시하여 액세스장치에 전송하고, 액세스장치는 비밀전송된 상기 고유키를 마스터키를 이용하여 복호하고, 복호된 고유키를 이용하여 암호를 실시한 상기 인증정보를 복호하여 상기 생성된 인증정보와 복호된 인증정보가 일치하는 경우에 기록매체장치가 정당성을 갖는다고 인증한다. 또 기록매체장치가 액세스장치를 인증하는 경우도 마찬가지이다. 이와 같이 구성되어 있으므로 장치는 접속된 상대의 장치가 정당한 장치인지 부정한 장치인지를 인증할 수 있다. 또 인증의 공정에 있어서 각 장치사이에서 암호화된 고유키의 전송과, 인증정보의 전송과, 암호화된 인증정보의 전송의 3회의 정보전송이 행해지므로 부정한 장치에 의한 인증순서를 모방하기 어렵다. 또 고유키의 암호와 인증정보의 암호의 두 가지의 암호방식이 이용되므로 부정한 장치에 의한 해독이 어렵다. 또 마스터키를 각 장치 사이에서 전송하지 않으므로 마스터키의 누설을 방지할 수 있다.

3. 그 밖의 실시예

또 본 발명을 상기 실시예에 기초하여 설명하였지만 본 발명은 상기 실시예에 한정되지 않는 것은 물론이다. 즉 이하와 같은 경우도 본 발명에 포함된다.

3.1. 디지털 저작물 보호시스템(100a)

본 발명에 관한 또 다른 실시예의 하나로서의 디지털 저작물 보호시스템 (100a)은 도 11의 블록도에 도시된 바와 같이 메모리카드(200a), 미디어고유키 정보작성장치(600), 메모리카드 기입기(300), 메모리카드 판독기(400)로 구성된다.

메모리카드 기입기(300), 메모리카드 판독기(400)는 각각 디지털 저작물 보호시스템(100)의 메모리카드 기입기(300), 메모리카드 판독기(400)와 거의 마찬가지이므로 설명은 생략한다.

메모리카드(200a)는 미디어고유키 정보작성장치(600)와 접속된다.

3. 1. 1 미디어고유키 정보작성장치(600)

미디어고유키 정보작성장치(600)는 마스터키 기억부(210b), 미디어고유키 기억부(220b), 변환부(230b), 미디어고유키 정보기억부(240b), 통신부(270b)로 구성된다.

마스터키 기억부(210b), 미디어고유키 기억부(220b), 변환부(230b), 미디어고유키 정보기억부(240b)에 대해서는, 각각 메모리카드(200)의 마스터키 기억부 (210), 미디어고유키 기억부(220), 변환부(230), 미디어고유키 정보기억부(240)와 같은 기능, 작용, 구성을 갖고 있고, 이하에서는 각각의 상위점을 중심으로 하여 설명한다.

(1) 마스터키 기억부(210b)

마스터키 기억부(210b)는 마스터키 기억부(210)와 마찬가지로 미리 하나의 마스터키 Mk를 기억하고 있다.

(2) 미디어고유키 기억부(220b)

미디어고유키 기억부(220b)는 통신부(270b)로부터 고유키 Ki를 수취하고, 수취한 고유키 Ki를 기억한다.

(3) 변환부(230b)

변환부(230b)는 변환부(230)와 마찬가지로 하여 미디어고유키 기억부(220b)에 기억되어 있는 고유키 Ki와 마스터키 기억부(210b)에 기억되어 있는 마스터키 Mk를 이용하여 암호화 고유키 Ji를 생성하고, 생성한 암호화 고유키 Ji를 미디어고유키 정보기억부(240b)로 출력한다.

(4) 미디어고유키 정보기억부(240b)

미디어고유키 정보기억부(240b)는 변환부(230b)로부터 암호화 고유키 Ji를 수취하고, 수취한 암호화 고유키 Ji를 기억한다.

(5) 통신부(270b)

통신부(270b)는 메모리카드(200a)의 통신부(270a)로부터 고유키 Ki를 수취하고, 수취한 고유키 Ki를 미디어고유키 기억부(220b)로 출력한다.

통신부(270b)는 미디어고유키 정보기억부(240b)로부터 암호화 고유키 Ji를 판독하고, 판독한 암호화 고유키 Ji를 메모리카드(200a)의 통신부(270a)로 출력한다.

3. 1. 2 메모리카드(200a)

메모리카드(200a)는 상기 도면에 도시된 바와 같이 마스터키 기억부(210), 미디어고유키 기억부(220), 미디어고유키 정보기억부(240a), 장치키 기억부(221), 역변환부(222), 장치키 정보기억부(223), 상호인증부(250), 암호화저작물 기억부(260), 통신부(270a), 제어부(280)로 구성된다.

메모리카드(200a)의 마스터키 기억부(210), 미디어고유키 기억부(220), 장치키 기억부(221), 역변환부(222), 장치키 정보기억부(223), 상호인증부(250), 암호화저작물 기억부(260), 제어부(280)는 각각 메모리카드(200)의 마스터키 기억부(210), 미디어고유키 기억부(220), 장치키 기억부(221), 역변환부(222), 장치키 정보기억부(223), 상호인증부(250), 암호화저작물 기억부(260), 제어부(280)와 같으므로 설명을 생략하고, 메모리카드(200a)의 미디어고유키 정보기억부(240a), 통신부(270a)에 대하여 메모리카드(200)의 미디어고유키 정보기억부(240), 통신부(270)와의 상위점을 중심으로 하여 설명한다.

(1) 미디어고유키 정보기억부(240a)

미디어고유키 정보기억부(240a)는 통신부(270a)로부터 암호화 고유키 Ji를 수취하고, 수취한 암호화 고유키 Ji를 기억한다.

(2) 통신부(270a)

통신부(270a)는 미디어고유키 기억부(220)로부터 고유키 Ki를 판독하고, 판독한 고유키 Ki를 미디어고유키 정보작성장치(600)의 통신부(270b)로 출력한다.

통신부(270a)는 미디어고유키 정보작성장치(600)의 통신부(270b)로부터 암호화 고유키 Ji를 수취하고, 수취한 암호화 고유키 Ji를 미디어고유키 정보기억부(240a)로 출력한다.

3. 1. 3 메모리카드(200a)가 미디어고유키 정보작성장치(600)에 장착된 경우의 동작

메모리카드(200a)가 미디어고유키 정보작성장치(600)에 장착된 경우의 동작에 대하여 도 12를 이용하여 설명한다.

메모리카드(200a)가 미디어고유키 정보작성장치(600)에 장착된 경우, 통신부(270a)는 미디어고유키 기억부(220)로부터 고유키 Ki를 판독하고, 판독한 고유키 Ki를 미디어고유키 정보작성장치(600)의 통신부(270b)를 통해 미디어고유키 기억부(220b)로 출력하고(단계 S211), 변환부(230b)는 미디어고유키 기억부(220b)에 기억되어 있는 고유키 Ki와 마스터키 기억부(210b)에 기억되어 있는 마스터키 Mk를 이용하여 암호화 고유키 Ji를 생성하고, 생성한 암호화 고유키 Ji를 미디어고유키 정보기억부(240b)로 출력하고(단계 S212), 통신부(270b)는 미디어고유키 정보기억부(240b)로부터 암호화 고유키 Ji를 판독하고, 판독한 암호화 고유키 Ji를 메모리카드(200a)의 통신부(270a)를 통해 미디어고유키 정보기억부(240a)로 출력한다 (단계 S213).

3. 1. 4 메모리카드(200a)가 메모리카드 기입기(300)에 장착된 경우의 상세한 인증동작

메모리카드(200a)가 메모리카드 기입기(300)에 장착된 경우의 상세한 인증동작에 대하여, 도 9와의 상위점에 관하여 도 12를 이용하여 설명한다.

인증동작의 상세한 것은 도 9에 도시된 단계 S139~S147이 도 12에 도시된 단계 S201~S206으로 치환된 것으로 된다.

난수발생부(251)는 난수 R_6을 생성하고(단계 S201), 통신부(270a)는 생성된 난수 R_6을 통신부(340)를 경유하여 암호부(332)로 출력하고(단계 S202), 암호부(332)는 마스터키 M_k를 암호알고리즘 E_2의 키로 하여 난수 R_6에 암호알고리즘 E_2를 실시하여 암호화난수 $E_2(M_k, R_6)$를 생성하고(단계 S203), 통신부(340)는 통신부(270)를 경유하여 암호화난수 $E_2(M_k, R_6)$를 복호부(253)로 출력하고(단계 S204), 복호부(253)는 마스터키 M_k를 복호알고리즘 D_2의 키로서 암호화난수 $E_2(M_k, R_6)$에 복호알고리즘 D_2를 실시하고, $D_2(M_k, E_2(M_k, R_6))$를 생성하고(단계 S205), 상호인증 제어부(254)는 난수 R_6과 $D_2(M_k, E_2(M_k, R_6))$를 비교하여 일치하면 메모리카드 기입기(300)는 정당한 장치라고 인식하고, 일치하지 않으면 메모리카드 기입기(300)는 부정한 장치라고 인식한다(단계 S206).

3. 1. 5 정리

이 실시예에 의하면 메모리카드(200a)가 사용자에게 배포, 판매되기 전에 메모리카드(200a)와 미디어고유키 정보작성장치(600)가 접속되고, 미디어고유키 정보작성장치(600)에 의해 생성된 암호화 고유키 Ki가 메모리카드(200a)에 기입된다.

이와 같이 구성함으로써 메모리카드(200)로부터 변환부(230)를 제거할 수 있고, 메모리카드(200a)에서는 메모리카드(200)와 비교하여 회로규모를 작게 할 수 있다는 효과가 있다.

또 기록매체장치가 액세스장치를 인증하는 경우에 기록매체장치는 난수로서 생성한 인증정보를 액세스장치에 전송하고, 액세스장치는 마스터키를 이용하여 상기 인증정보에 암호를 실시하여 기록매체장치에 전송하고, 기록매체장치는 암호가 실시된 인증정보를 마스터키를 이용하여 복호하며, 상기 생성된 인증정보와 복호된 인증정보가 일치하는 경우에 액세스장치가 정당성을 갖는다고 인증한다. 이와 같이 구성되어 있으므로 디지털 저작물 보호시스템(100)과 비교하면 장치의 인증공정을 보다 간소하게 할 수 있다. 이 경우에도 마스터키를 각 장치 사이에서 전송하지 않으므로 마스터키의 누설을 방지할 수 있다.

3. 2 다른 디지털 저작물 보호시스템

디지털 저작물 보호시스템(100)에서는 메모리카드(200), 메모리카드 기입기(300), 메모리카드 판독기(400)는 동일한 마스터키를 갖고, 마스터키를 공통키 암호알고리즘 또는 공통키 복호알고리즘의 키로 하고 있지만, 마스터키 대신 메모리카드(200)는 공개키암호의 일종인 RSA 암호의 공개키 K_o를 갖고, 메모리카드 기입기(300), 메모리카드 판독기(400)는 그 비밀키 K_o를 갖는다고 해도 된다.

여기에서 공개키 K_o와 비밀키 K_o는 다음과 같이 하여 결정된다. p, q를 각각 약 160자리수 정도의 10진수로 하고, 그 곱을 n으로 하고, 정수 L을 p-1 및 q-1의 최소공배수로 하고, 수 e 및 d를 mod L 하에서 서로 역수가 되는 수로 한다. 즉 $e \cdot d = 1 \pmod{L}$로 한다. 또 공개키 K_o를 n 및 e로 하고, 비밀키 K_o를 d로 한다. 변환부에서는 입력 M에 대하여 mod n 하에서 M^e(M의 e승)의 연산을 행하여 변환결과 C를 구하고, 역변환부에서는 입력 C에 대하여 C^d(C의 d승)의 연산을 행한다. mod n 하에서 $C^d = (M^e)^d = M^{ed} = M$이므로 역변환을 잘 할 수 있는 것을 알 수 있다.

공개키 K_o는 상기에 나타낸 바와 같이 하여 미리 다른 공개키 생성장치에 의해 생성되고, 생성된 공개키 K_o가 메모리카드(200)에 송신되어 있다.

(메모리카드(200)가 메모리카드 기입기(300)에 장착된 경우의 상세한 인증동작)

다음으로 메모리카드(200)가 메모리카드 기입기(300)에 장착된 경우의 상세한 인증동작에 대하여 도 13을 이용하여 설명한다. 또 도 10과 같은 부호를 갖는 단계에 대해서는 같은 동작이므로 설명을 생략한다.

공개키 생성장치는 미리 메모리카드 기입기(300)로부터 비밀키 K_o를 판독하고, 판독한 비밀키 K_o를 기초로 하여 공개키 암호알고리즘을 이용하여 공개키 K_o를 생성하고, 생성한 공개키 K_o를 메모리카드(200)에 송신하고, 메모리카드(200)는 송신된 공개키 K_o를 기억한다(단계 S301).

변환부(230)는 공개키 K_o를 암호알고리즘 E_i의 키로 하여 고유키 Ki에 암호알고리즘 E_i를 실시하여 암호화 고유키 $E_i(K_o, Ki)$를 생성하고(단계 S302), 통신부 (270)는 암호화 고유키 $E_i(K_o, Ki)$를 통신부(340)를 경유하여 역변환부(321)로 출력하고(단계 S303), 역변환부(321)는 비밀키 K_o를 복호알고리즘 D_i의 키로 하여 암호화 고유키 $E_i(K_o, Ki)$에 복호알고리즘 D_i를 실시하여 고유키 $Ki = D_i(K_o, E_i(K_o, Ki))$를 생성한다(단계 S304).

여기에서 암호알고리즘 E_i 및 복호알고리즘 D_i는 RSA에 의한 알고리즘이다.

공개키와 비밀키가 이와 같이 구성되어 있으므로 비밀키 d로부터 공개키 e를 계산할 수 없다. 왜냐하면 비밀키 d를 알고 있을 때 이제부터 e를 구하기 위해서는 mod L이 알려져 있어야 하는데, L은 p-1과 q-1의 최소공배수이므로 p와 q의 곱을 알고 있는 것만으로는 구할 수 없기 때문이다. 이로 인하여 카드 판독기 또는 카드 기입기에 존재하는 비밀키 d가 가령 폭로되었다고 해도 이제부터 공개키 e를 구할 수 없으므로 메모리카드의 위조가 곤란하다는 효과가 있다.

또 암호알고리즘 E_i 및 복호알고리즘 D_i는 RSA 암호에 한정되는 것은 아니고, 다른 암호알고리즘이어도 된다.

3. 3 다른 디지털 저작물 보호시스템

상기 「3.2. 다른 디지털 저작물 보호시스템」에 나타내는 디지털 저작물 보호시스템에서는 메모리카드(200)는 공개키 K_o를 갖고, 메모리카드 기입기(300), 메모리카드 판독기(400)는 비밀키 K_o를 갖는다고 하고 있지만, 또 다른 디지털 저작물 보호시스템에서는 메모리카드(200)는 공개키 암호계의 일종인 타원곡선상의 회복형 서명 비밀키 K_o를 갖고, 메모리카드 기입기(300), 메모리카드 판독기(400)는 공개키 K_o를 갖는다고 해도 된다. 여기에서 공개키 K_o와 비밀키 K_o는 다음과 같이 하여 결정된다.

비밀키 K_o로서 스칼라 x가 선택된다. 공개키 K_o는 타원곡선상의 기점을 G로 하고, $G + G + \cdots + G$(x회의 가산)의 점으로 한다. 변환처리로서 비밀키 K_o를 이용한 회복형 서명변환을 이용하고, 역변환처리로서 공개키 K_o를 이용하여 회복형 서명검증변환을 이용한다. 또 회복형 서명에 대해서는 「A message recovery signature scheme equivalent to DSA over elliptic curves」(Atsuko Miyaji저, Advances in Cryptology-Proceedings of ASIACRYPT'96, Lecture Notes in Computer Science, 1163(1996), Springer-Verlag, 1-

14)에 기재되어 있으므로 설명은 생략한다.

이 때 공개키 K_p는 메모리카드(200)가 갖는 비밀키 K_s를 기초로 하여 공개키 암호알고리즘을 이용하여, 미리 다른 공개키 생성장치에 의해 생성되고, 생성된 공개키 K_p가 메모리카드 기입기(300)에 송신되어 있다.

변환부(230)는 비밀키 K_s를 암호알고리즘 E_1의 키로 하여 고유키 K_1에 암호알고리즘 E_1를 실시하여 암호화 고유키 $E_1(K_s, K_1)$를 생성한다. 또 역변환부(321)는 공개키 K_p를 복호알고리즘 D_1의 키로 하여 암호화 고유키 $E_1(K_s, K_1)$에 복호알고리즘 D_1를 실시하여 고유키 $K_1 = D_1(K_p, E_1(K_s, K_1))$를 생성한다.

공개키 K_p와 비밀키 K_s가 이와 같이 구성되어 있으므로 공개키 K_p로부터 비밀키 K_s를 구하는 것이 계산양적으로 매우 어려워진다. 따라서 메모리카드에 비해 내부해석의 위험성이 상대적으로 높다고 생각되는 메모리 기입기 또는 메모리 판독기에 공개키를 부여하고, 메모리카드에 비밀키를 부여하는 구성이 운용시스템 전체의 기밀성을 높이는 효과를 가진다.

또 타원곡선 암호계와 같은 이산대수문제에 안전성의 근거를 갖는 공개키 암호계에서는 비밀키로부터 공개키가 구해지는 것에 주의하기 바란다.

3. 4 다른 디지털 저작물 보호시스템

본 발명에 관한 또 다른 실시예의 하나로서의 디지털 저작물 보호시스템 (100c)은 도 14, 도 15, 도 16의 블록도에 각각 나타내는 메모리카드(200c), 메모리카드 기입기(300c), 메모리카드 판독기(400c)로 구성된다.

메모리카드(200c)는 도시하지 않은 마스터키 선택장치에 장착된다. 또 메모리카드 기입기(300c), 메모리카드 판독기(400c)는 마스터키 선택장치에 접속된다.

3. 4. 1 마스터키 선택장치

마스터키 선택장치에 메모리카드(200c)가 장착되는 경우에는 마스터키 선택장치는 메모리카드(200c)의 통신부(270)와 접속된다.

마스터키 선택장치와 메모리카드 기입기(300c)가 접속되는 경우에는 마스터키 선택장치는 메모리카드 기입기(300c)의 통신부(340)와 접속된다.

마스터키 선택장치와 메모리카드 판독기(400c)가 접속되는 경우에는 마스터키 선택장치는 메모리카드 판독기(400c)의 통신부(440)와 접속된다.

마스터키 선택장치는 메모리카드(200c), 메모리카드 기입기(300c) 또는 메모리카드 판독기(400c)와 접속되는 경우에 접속되는 메모리카드(200c)의 통신부(270), 메모리카드 기입기(300c)의 통신부(340) 또는 메모리카드 판독기(400c)의 통신부(440)에 대하여 패스워드를 출력한다.

패스워드는 복수의 마스터키 중 하나에 대응한다.

3. 4. 2 메모리카드(200c)

메모리카드(200c)는 메모리카드(200)에 추가로 마스터키 선택부(215)를 구비한다. 메모리카드(200c)의 그 밖의 구성요소는 메모리카드(200)와 마찬가지이다. 이하에서 메모리카드(200)와의 상위점을 중심으로 하여 설명한다.

마스터키 기억부(210)는 복수의 마스터키를 미리 기억하고 있다.

메모리카드(200c)가 마스터키 선택장치에 장착되었을 때 메모리카드(200c)는 마스터키 선택장치와 통신부(270)를 통해 접속된다.

통신부(270)는 마스터키 선택장치로부터 패스워드를 수취하고, 수취한 패스워드를 마스터키 선택부(215)에 출력한다.

마스터키 선택부(215)는 통신부(271)로부터 수취한 패스워드를 이용하여 상기 패스워드에 대응하는 하나의 마스터키를 마스터키 기억부(210)로부터 선택하고, 선택한 마스터키를 마스터키 기억부(210)로 출력한다.

마스터키 기억부(210)는 선택된 마스터키에 선택된 것을 나타내는 선택마크를 붙여 기억한다.

변환부(230), 역변환부(222)는 상기 선택마크가 첨부된 마스터키를 판독한다.

3. 4. 3 메모리카드 기입기(300c), 메모리카드 판독기(400c)

메모리카드 기입기(300c)는 메모리카드 기입기(300)에 추가로 마스터키 선택부(315)를 구비한다. 메모리카드 기입기(300c)의 그 밖의 구성요소는 메모리카드 기입기(300)와 마찬가지이다.

마스터키 기억부(313)는 복수의 마스터키를 미리 기억하고 있다.

메모리카드(200c)와 마찬가지로, 통신부(340)는 마스터키 선택장치로부터 패스워드를 수취하고, 마스터키 선택부(315)에 출력하고, 마스터키 선택부(315)는 수취한 패스워드를 이용하여 대응하는 하나의 마스터키를 마스터키 기억부(313)로부터 선택하고, 마스터키 기억부(313)는 선택된 마스터키에 선택된 것을 나타내는 선택마크를 붙여 기억한다.

변환부(311), 역변환부(321)는 상기 선택마크가 부착된 마스터키를 판독한다.

메모리카드 판독기(400c)에 대해서도 메모리카드 기입기(300c)와 마찬가지이다.

3. 4. 4 정리

본 실시예에 나타내는 디지털 저작물 보호시스템(100c)은 다른 복수의 운용시스템에서 적용된다. 운용시스템의 일례로서 음악배포시스템이 있고, 이 음악배포시스템은 A사, B사, C사의 3사가 공동으로 운영한다. 또 다른 운용시스템의 일례로서, 영화임대제도가 있고, 이 영화임대제도는 X사, Y사, Z사가 공동으로 운영한다.

하나의 운용시스템에서는 하나의 동일한 마스터키가 이용되고, 다른 운용시스템에서는 다른 마스터키가 이용된다. 예를 들면 상기 음악배포 시스템에는 마스터키 M1이 이용되고, 상기 영화임대제도에는 마스터키 M1과는 다른 마스터키 M2가 이용된다.

디지털 저작물 보호시스템(100c)이 적용되는 바람직한 운용시스템에서는 라이센스조직과 제조업자와 사용자의 3자가 존재한다. 상기 라이센스조직은 운용시스템의 규격을 결정함과 동시에 마스터키 등의 비밀정보의 비밀성을 확보하는 입장에 있고, 각 제조업자에게 라이센스의 허락을 부여하고, 상기 제조업자는 라이센스조직으로부터 허락을 받아 소정 규격의 기기를 제조하여 사용자에게 제공하는 입장에 있고, 상기 사용자는 개개의 기기를 이용한다.

메모리카드, 메모리카드 기입기 또는 메모리카드 판독기 등의 장치의 제조에 있어서 제조업자에 대하여 마스터키를 누설하지 않도록 완전한 기밀성 조건을 부과하는 것은 어렵다. 또 메모리카드 기입기 또는 메모리카드 판독기는 메모리카드보다 상대적으로 해석이 용이하다고 생각된다.

따라서 마스터키의 누설 가능성을 가능한 한 낮게 하고, 또 마스터키의 선택을 포함하는 장치의 제조비용이나 운용시스템의 유지비용을 낮게 하기 위해 메모리카드의 마스터키의 선택은 제조업자에 맡기고, 메모리카드 기입기 및 메모리카드 판독기의 마스터키의 선택은 라이센스 조직이 행하도록 하고 있다.

이로 인하여 메모리카드용 마스터키 선택장치(901)와, 메모리카드 기입기용 마스터키 선택장치(902)와, 메모리카드 판독기용 마스터키 선택장치(903)가 존재하며, 마스터키 선택장치(901)는 제조업자의 가까이에 있고, 마스터키 선택장치(902)와 마스터키 선택장치(903)는 라이센스조직의 가까이에 있어 제조업자에게는 양도되지 않는다.

제조업자에 의해 메모리카드가 제조되었을 때 메모리카드는 복수의 마스터키를 갖고 있고, 그 중 하나를 마스터키 선택장치(901)에 의해 선택한다. 한편 메모리카드 기입기 또는 메모리카드 판독기에는 미리 라이센스조직이 소유하는 마스터키 선택장치(902, 903)를 이용하여 선택한 결과의 마스터키만이 기록되어 있다.

이와 같이 기록매체장치 및 액세스장치는 복수의 마스터키를 갖고 있으므로 복수의 다른 디지털 저작물 운용시스템에서도 적용할 수 있다.

또 하나의 운용시스템에 있어서는 하나의 동일한 마스터키가 이용되고, 다른 운용시스템에 있어서는 다른 마스터키가 이용되므로 어떤 운용시스템의 마스터키가 폭로되었다고 해도 다른 운용시스템에 영향을 주지 않아 안정성이 높은 기밀성 시스템이 실현된다는 효과가 있다.

3. 5. 다른 디지털 저작물 보호시스템

본 발명에 관한 또 다른 실시예의 하나로서의 디지털 저작물 보호시스템 (100d)은 도 17에 도시된 메모리카드(200d), 메모리카드 기입기(300d), 도시하지 않은 메모리카드 판독기(400d)로 구성된다.

메모리카드(200d), 메모리카드 기입기(300d), 메모리카드 판독기(400d)는 각각 메모리카드(200), 메모리카드 기입기(300), 메모리카드 판독기(400)와 같은 구성이므로 이하에서는 상위점을 중심으로 하여 설명한다.

3. 5. 1 메모리카드(200d)

메모리카드(200d)는 메모리카드(200)와 비교하면 서브그룹키 기억부(290d), 변환부(291d)를 추가로 갖고 있는 점이 다르다. 또 메모리카드(200d)의 그 밖의 구성요소에 대해서는 이하에 설명이 없는 한 메모리카드(200)의 구성요소와 마찬가지이며, 설명을 생략한다.

(1) 서브그룹키 기억부(290d)

서브그룹키 기억부(290d)는 미리 하나의 서브그룹키 Gjk를 기억하고 있다. 서브그룹키 Gjk는 56비트의 비트열로 이루어진다.

하나의 디지털 저작물 운용시스템을 복수의 단체가 운영하는 경우, 이들의 단체의 수만큼 다른 서브그룹키가 존재하고, 이들의 다른 서브그룹키가 각각 상기 복수의 단체에 할당된다.

예를 들면 디지털 저작물 운용시스템은 음악을 배포하는 음악배포 시스템이고, 이 음악배포 시스템을 A사, B사, C사의 3사가 공동으로 운영하는 경우에 3가지의 다른 서브그룹키가 존재하고, 이들의 다른 3가지의 서브그룹키가 각각 A사, B사, C사의 3사에 할당된다.

(2) 변환부(291d)

변환부(291d)는 서브그룹키 기억부(290d)에 기억되어 있는 하나의 서브그룹키 Gjk를 판독하고, 미디어고유키 기억부(220)에 기억되어 있는 하나의 고유키 Ki를 판독한다.

변환부(291d)는 판독한 하나의 서브그룹키 Gjk와, 판독한 하나의 고유키 Ki 에 대하여 소정의 연산을 실시하고, 변형키를 생성한다.

여기에서 소정의 연산이란 일례로서 배타적 논리합이다.

(변형키) = (서브그룹키 Gjk) EOR(고유키 Ki)

여기에서 EOR은 배타적 논리합을 나타내는 연산이다.

변환부(291d)는 생성한 변형키를 변환부(230)로 출력한다.

(3) 변환부(230)

변환부(230)는 미디어고유키 기억부(220)에 기억되어 있는 고유키 Ki를 판독하고, 판독한 고유키 Ki에 암호알고리즘 E_i을 실시하여 암호화 고유키 Ji를 생성하는 대신 변환부(291d)로부터 변형키를 수취하고, 수취한 변형키에 암호알고리즘 E_i을 실시하여 암호화 고유키 Ji를 생성한다.

3. 5. 2 메모리카드 기입기(300d)

메모리카드 기입기(300d)는 메모리카드 기입기(300)와 비교하면 추가로 서브그룹키 기억부(390d), 역변환부(391d)를 갖고 있는 점이 다르다. 또 메모리카드 기입기(300d)의 그 밖의 구성요소에 대해서는 이하에 설명이 없는 한 메모리카드 기입기(300)의 구성요소와 마찬가지이며, 설명을 생략한다.

(1) 서브그룹키 기억부(390d)

서브그룹키 기억부(390d)는 서브그룹키 기억부(290d)와 마찬가지로 미리 하나의 서브그룹키 Gjk를 기억하고 있다. 서브그룹키 Gjk는 56비트의 비트열로 이루어진다.

서브그룹키 Gjk에 대해서는 서브그룹키 기억부(290d)에 기억되어 있는 서브그룹키 GjK와 같으므로 설명을 생략한다.

(2) 역변환부(321)

역변환부(321)는 판독한 암호화 고유키 Ji에 복호알고리즘 D_i을 실시하여 고유키 K'i를 생성하고, 생성한 고유키 K'i를 미디어고유키 기억부(323)로 출력하는 대신 판독한 암호화 고유키 Ji에 복호알고리즘 D_i을 실시하여 변형키를 생성하고, 생성한 변형키를 역변환부(391d)로 출력한다.

(3) 역변환부(391d)

역변환부(391d)는 서브그룹키 기억부(390d)에 기억되어 있는 하나의 서브그룹키 Gjk를 판독하고, 역변환부(321)로부터 변형키를 수취한다.

역변환부(391d)는 판독한 하나의 서브그룹키 GjK와, 수취한 변형키에 대하여 변환부(291d)에서 실시되는 소정 연산의 역연산을 실시하여 고유키 K'i를 생성한다.

역변환부(391d)는 생성한 고유키 K'i를 미디어고유키 기억부(323)로 출력한다.

(4) 미디어고유키 기억부(323)

미디어고유키 기억부(323)는 역변환부(391d)로부터 고유키 K'i를 수취하고, 수취한 고유키 K'i를 기억한다.

3. 5. 3 메모리카드 판독기(400d)

메모리카드 판독기(400d)는 메모리카드 판독기(400)와 비교하면, 추가로 서브그룹키 기억부(490d), 역변환부(491d)를 갖고 있는 점이 다르다. 여기에서 서브그룹키 기억부(490d), 역변환부(491d)는 각각 서브그룹키 기억부(390d), 역변환부 (391d)와 마찬가지이므로 설명을 생략한다. 또 메모리카드 판독기(400d)의 역변환부(421)와 미디어고유키 기억부(423)는 각각 메모리카드 기입기(300d)의 역변환부 (321)와 미디어고유키 기억부(323)와 마찬가지이고, 메모리카드 판독기(400d)의 그 밖의 구성요소에 대해서는 메모리카드 판독기(400)의 구성요소와 마찬가지이므로 설명을 생략한다.

3. 5. 4 디지털 저작물 보호시스템(100d)의 동작

디지털 저작물 보호시스템(100d)의 동작에 대하여 설명한다.

메모리카드(200d)가 메모리카드 기입기(300d)에 장착된 경우의 개요동작 및 메모리카드(200d)가 메모리카드 판독기(400d)에 장착된 경우의 개요동작에 대해서는 디지털 저작물 보호시스템(100)과 마찬가지이므로 설명을 생략한다.

다음으로 메모리카드(200d)가 메모리카드 기입기(300d)에 장착된 경우의 상세한 인증동작에 대하여 도 18을 이용하여 디지털 저작물 보호시스템(100)의 경우와의 상위점을 중심으로 설명한다.

단계 S150d에서 변환부(291d)는 서브그룹키 기억부(290d)에 기억되어 있는 하나의 서브그룹키 Gjk를 판독하고, 미디어고유키 기억부(220)에 기억되어 있는 하나의 고유키 Ki를 판독하고, 판독한 하나의 서브그룹키 GjK와, 판독한 하나의 고유키 Ki에 대하여 소정의 연산을 실시하여 변형키 HJk를 생성한다.

단계 S130에 있어서, 변환부(230)는 마스터키 Mk를 암호알고리즘 E_i의 키로서, 변형키 HJk에 암호알고리즘 E_i을 실시하여 암호화 고유키 E_i(Mk, HJk)을 생성한다.

단계 S132에 있어서, 역변환부(321)는 마스터키 Mk를 복호알고리즘 D_i의 키로 하여 암호화 고유키 E_i(Mk, HJk)에 복호알고리즘 D_i을 실시하여 변형키 D_i(Mk, E_i(Mk, HJk))을 생성한다.

단계 S151d에서 역변환부(391d)는 서브그룹키 기억부(390d)에 기억되어 있는 하나의 서브그룹키 Gjk를 판독하고, 역변환부(321)로부터 변형키 D_i(Mk, E_i(Mk, HJk))을 수취하고, 판독한 하나의 서브그룹키 GjK와, 수취한 변형키 D_i(Mk, E_i(Mk, HJk))에 대하여 변환부(291d)에서 실시되는 소정 연산의 역연산을 실시하여 고유키 K'i를 생성한다.

또 메모리카드(200d)가 메모리카드 판독기(400d)에 장착된 경우의 상세한 인증동작에 대해서는 상기와 마찬가지이므로 설명을 생략한다.

3. 5. 5 정리

하나의 디지털 저작물 운용시스템을 복수의 단체가 운영하는 경우, 이들 단체의 수만큼 다른 서브그룹키가 존재하고, 이들의 다른 서브그룹키가 각각 상기 복수의 단체에 할당되므로 각 단체는 독자적인 서비스 제공이 가능해진다.

예를 들면 디지털 저작물 운용시스템은 음악을 배포하는 음악배포 시스템이고, 이 음악배포 시스템을 A사, B사, C사의 3사가 공동으로 운영하는 경우에 3가지의 다른 서브그룹키가 존재하고, 이들의 다른 3가지의 서브그룹키가 각각 A사, B사, C사의 3사에게 할당되므로 A사, B사, C사는 각각 독자적인 음악배포 서비스를 제공할 수 있게 된다.

또 메모리카드의 기억용량은 한정되어 있으므로 메모리카드에 기억할 수 있는 마스터키의 수에는 제한이 있는 경우가 많고 마스터키와 서브그룹의 조합에 의해 이용할 수 있는 키의 수를 늘릴 수 있다는 효과가 있다.

또 디지털 저작물 보호시스템(100d)에서 변환부(291d)에 대하여 변환처리를 행하게 하지 않고, 변환부(230)에 대하여 미디어고유키 기록부(220)에 기억되어 있는 고유키를 변환시키는 제어부 및 역변환부(391d)에 대하여 역변환처리를 행하게 하지 않고, 역변환부(321)에 대하여 미디어고유키 정보기록부(320)에 기억되어 있는 암호화 고유키를 역변환시키는 제어부를 설치함으로써 각 단체마다 서브그룹키를 할당한 후 추가로 하나의 디지털 저작물 운용시스템에 하나의 마스터키를 할당하고, 각 단체의 공통 서비스를 제공할 수도 있다.

3. 6 다른 디지털 저작물 보호시스템

본 발명에 관한 또 다른 실시예의 하나로서의 디지털 저작물 보호시스템 (100e)은 도 19에 도시된 메모리카드(200e), 메모리카드 기입기(300e), 도시하지 않는 메모리카드 판독기(400e)로 구성된다.

메모리카드(200e), 메모리카드 기입기(300e), 메모리카드 판독기(400e)는 각각 메모리카드(200), 메모리카드 기입기(300), 메모리카드 판독기(400)와 같은 구성이므로 이하에서는 상위점을 중심으로 하여 설명한다.

3. 6. 1 메모리카드(200e)

메모리카드(200e)는 메모리카드(200)와 비교하면 추가로 서브그룹키 기억부 (290e), 변환부(291e)를 갖고 있는 점이 다르다. 또 메모리카드(200e)의 그 밖의 구성요소에 대해서는 이하에 설명이 없는 한 메모리카드(200)의 구성요소와 마찬가지이며, 설명을 생략한다.

(1) 서브그룹키 기억부(290e)

서브그룹키 기억부(290e)는 미리 하나의 서브그룹키 Gjk를 기억하고 있다. 서브그룹키 Gjk는 56비트의 비트열로 이루어진다.

서브그룹키는 서브그룹키 기억부(290d)의 서브그룹키와 같으므로 설명은 생략한다.

(2) 변환부(291e)

변환부(291e)는 서브그룹키 기억부(290e)에 기억되어 있는 하나의 서브그룹키 Gjk를 판독하고, 미디어고유키 정보기억부(240)에 기억되어 있는 암호화 고유키 Ji를 판독한다.

변환부(291e)는 판독한 하나의 서브그룹키 Gjk와, 판독한 하나의 암호화 고유키 Ji에 대하여 소정의 연산을 실시하고 변형키를 생성한다.

여기에서 소정의 연산이란 변환부(291d)에서 이용되는 소정의 연산과 같은 연산이다.

변환부(291e)는 생성된 변형키를 통신부(270)로 출력한다.

(3) 통신부(270)

통신부(270)는 미디어고유키 정보기억부(240)로부터 암호화 고유키 Ji를 판독하고, 판독한 암호화 고유키 Ji를 메모리카드 기입기(300)의 통신부(340) 또는 메모리카드 판독기(400)의 통신부(440)로 출력하는 대신 변환부(291e)로부터 변형키를 수취하고, 수취한 변형키를 메모리카드 기입기(300e)의 통신부(340) 또는 메모리카드 판독기(400e)의 통신부(440)로 출력한다.

3. 6. 2 메모리카드 기입기(300e)

메모리카드 기입기(300e)는 메모리카드 기입기(300)와 비교하면 추가로 서브그룹키 기억부(390e), 역변환부(391e)를 갖고 있는 점이 다르다. 또 메모리카드 기입기(300e)의 그 밖의 구성요소에 대해서는 이하에 설명이 없는 한 메모리카드 기입기(300)의 구성요소와 마찬가지이며 설명을 생략한다.

(1) 서브그룹키 기억부(390e)

서브그룹키 기억부(390e)는 서브그룹키 기억부(290e)와 마찬가지로 미리 하나의 서브그룹키 Gjk를 기억하고 있다. 서브그룹키 Gjk는 56비트의 비트열로 이루어진다.

서브그룹키 Gjk에 대해서는 서브그룹키 기억부(290e)에 기억되어 있는 서브그룹키 Gjk와 같으므로 설명을 생략한다.

(2) 통신부(340)

통신부(340)는 메모리카드(200)의 통신부(270)로부터 암호화 고유키 JI를 수취하고, 수취한 암호화 고유키 JI를 미디어고유키 정보기억부(320)로 출력하는 대신 메모리카드(200e)의 통신부(270)로부터 변형키를 수취하고, 수취한 변형키를 역변환부(391e)로 출력한다.

(3) 역변환부(391e)

역변환부(391e)는 서브그룹키 기억부(390e)에 기억되어 있는 하나의 서브그룹키 Gjk를 판독하고, 통신부(340)로부터 변형키를 수취한다.

역변환부(391e)는 판독한 하나의 서브그룹키 Gjk와, 수취한 변형키에 대하여 변환부(291e)에서 실시되는 소정 연산의 역연산을 실시하고, 암호화 고유키 JI를 생성한다.

역변환부(391d)는 생성한 암호화 고유키 JI를 미디어고유키 정보기억부(320)로 출력한다.

3. 6. 3 메모리카드 판독기(400e)

메모리카드 판독기(400e)는 메모리카드 판독기(400)와 비교하면, 추가로 서브그룹키 기억부(490e), 역변환부(491e)를 갖고 있는 점이 다르다. 여기에서, 서브그룹키 기억부(490e), 역변환부(491e)는 각각 서브그룹키 기억부(390e), 역변환부 (391e)와 마찬가지이므로 설명을 생략한다. 또 메모리카드 판독기(400e)의 통신부 (440)는 메모리카드 기입기(300e)의 통신부(340)와 마찬가지이며, 메모리카드 판독기(400e)의 그 밖의 구성요소에 대해서는 메모리카드 판독기(400)의 구성요소와 마찬가지이므로 설명을 생략한다.

3. 6. 4 디지털 저작물 보호시스템(100e)의 동작

디지털 저작물 보호시스템(100e)의 동작에 대하여 설명한다.

메모리카드(200e)가 메모리카드 기입기(300e)에 장착된 경우의 개요동작 및 메모리카드(200e)가 메모리카드 판독기(400e)에 장착된 경우의 개요동작에 대해서는 디지털 저작물 보호시스템(100)과 마찬가지이므로 설명을 생략한다.

다음으로 메모리카드(200e)가 메모리카드 기입기(300e)에 장착된 경우의 상세한 인증동작에 대하여 도 20을 이용하여 디지털 저작물 보호시스템(100)의 경우와의 상위점을 중심으로 설명한다.

단계 S150e에서 변환부(291e)는 서브그룹키 기억부(290e)에 기억되어 있는 하나의 서브그룹키 Gjk를 판독하고, 미디어고유키 정보기억부(240)에 기억되어 있는 암호화 고유키 JI를 판독하고, 판독한 하나의 서브그룹키 Gjk와, 판독한 하나의 암호화 고유키 JI에 대하여 소정 연산을 실시하여 변형키를 생성하고, 생성한 변형키를 통신부(270)로 출력한다.

단계 131에서 통신부(270)는 변환부(291e)로부터 변형키를 수취하고, 수취한 변형키를 메모리카드 기입기(300e)의 통신부(340)로 출력하고, 통신부(340)는 메모리카드(200e)의 통신부(270)로부터 변형키를 수취하고, 수취한 변형키를 역변환부 (391e)로 출력한다.

단계 S151e에서 역변환부(391e)는 서브그룹키 기억부(390e)에 기억되어 있는 하나의 서브그룹키 Gjk를 판독하고, 통신부(340)로부터 변형키를 수취하고, 판독한 하나의 서브그룹키 Gjk와, 수취한 변형키에 대하여 변환부(291e)에서 실시되는 소정 연산의 역연산을 실시하여 암호화 고유키 JI를 생성한다.

또 메모리카드(200e)가 메모리카드 판독기(400e)에 장착된 경우의 상세한 인증동작에 대해서는 상기와 마찬가지이므로 설명을 생략한다.

3. 6. 5 정리

디지털 저작물 보호시스템(100d)과 마찬가지로 하나의 디지털 저작물 운용시스템을 복수의 단체가 운영하는 경우, 이들 단체의 수만큼 다른 서브그룹키가 존재하고, 이들의 다른 서브그룹키가 각각 상기 복수의 단체에 할당되므로 각 단체는 독자적인 서비스 제공이 가능해진다.

또 메모리카드의 기억용량은 한정되어 있으므로 메모리카드에 기억할 수 있는 마스터키의 수에는 제한이 있는 경우가 많고, 마스터키와 서브그룹키의 조합에 의해 이용할 수 있는 키의 수를 늘릴 수 있다는 효과가 있다.

또 디지털 저작물 보호시스템(100e)에서 변환부(291e)에 대하여 변환처리를 하게 하지 않고, 변환부(230)에 대하여 미디어고유키 기록부(220)에 기억되어 있는 고유키를 변환시키는 제어부 및 역변환부(391e)에 대하여 역변환처리를 하게 하지 않고, 역변환부(321)에 대하여 미디어고유키 정보기록부(320)에 기억되어 있는 암호화 고유키를 역변환시키는 제어부를 설치함으로써 각 단체마다 서브그룹키를 할당한 후 다시 하나의 디지털 저작물 운용시스템에 하나의 마스터키를 할당하고, 각 단체의 공통의 서비스를 제공할 수도 있다.

3. 7 다른 디지털 저작물 보호시스템

본 발명에 관한 또 다른 실시예의 하나로서의 디지털 저작물 보호시스템 (100f)은 도 21에 도시된 메모리카드(200f), 메모리카드 기입기(300f), 도시하지 않는 메모리카드 판독기(400f)로 구성된다.

메모리카드(200f), 메모리카드 기입기(300f), 메모리카드 판독기(400f)는, 각각 메모리카드(200), 메모리카드 기입기(300), 메모리카드 판독기(400)와 같은 구성이므로 이하에서는 상위점을 중심으로 하여 설명한다.

3. 7. 1 메모리카드(200f)

메모리카드(200f)는 메모리카드(200)와 비교하면, 추가로 서브그룹키 기억부 (290f), 변환부(291f)를 갖고 있는 점이 다르다. 또 메모리카드(200f)의 그 밖의 구성요소에 대해서는 이하에 설명이 없는 한 메모리카드(200)의 구성요소와 마찬가지이며, 설명을 생략한다.

(1) 서브그룹키 기억부(290f)

서브그룹키 기억부(290f)는 미리 하나의 서브그룹키 Gjk를 기억하고 있다. 서브그룹키 Gjk는 56비트의 비트열로 이루어진다.

서브그룹키는 서브그룹키 기억부(290d)의 서브그룹키와 같으므로 설명은 생략한다.

(2) 변환부(291f)

변환부(291f)는 서브그룹키 기억부(290f)에 기억되어 있는 하나의 서브그룹키 Gjk를 판독하고, 마스터키 기억부(210)에 기억되어 있는 마스터키 Mk를 판독한다.

변환부(291f)는 판독한 하나의 서브그룹키 Gjk와, 판독한 하나의 마스터키 Mk에 대하여 소정의 연산을 실시하여 변형키를 생성한다.

여기에서 소정의 연산이란 변환부(291d)에서 이용되는 소정의 연산과 같은 연산이다.

변환부(291f)는 생성한 변형키를 변환부(230)로 출력한다.

(3) 변환부(230)

변환부(230)는 마스터키 기억부(210)에 기억되어 있는 마스터키 Mk를 판독하고, 상기 판독한 마스터키 Mk를 암호알고리즘 E_i의 키로서 판독한 고유키 Ki에 암호알고리즘 E_i을 실시하여 암호화 고유키 Ji를 생성하는 대신 변환부(291f)로부터 변형키를 수취하고, 상기 수취한 변형키를 암호알고리즘 E_i의 키로 하여 판독한 고유키 Ki에 암호알고리즘 E_i을 실시하고 암호화 고유키 Ji를 생성한다.

3.7.2 메모리카드 기입기(300f)

메모리카드 기입기(300f)는 메모리카드 기입기(300)와 비교하면 추가로 서브그룹키 기억부(390f), 역변환부(391f)를 갖고 있는 점이 다르다. 또 메모리카드 기입기(300f)의 그 밖의 구성요소에 대해서는 이하에 설명이 없는 한 메모리카드 기입기(300)의 구성요소와 마찬가지이며, 설명을 생략한다.

(1) 서브그룹키 기억부(390f)

서브그룹키 기억부(390f)는 서브그룹키 기억부(290f)와 마찬가지로 미리 하나의 서브그룹키 Gjk를 기억하고 있다. 서브그룹키 Gjk는 56비트의 비트열로 이루어진다.

서브그룹키 Gjk에 대해서는 서브그룹키 기억부(290f)에 기억되어 있는 서브그룹키 Gjk와 같으므로 설명을 생략한다.

(2) 역변환부(391f)

역변환부(391f)는 서브그룹키 기억부(390f)에 기억되어 있는 하나의 서브그룹키 Gjk를 판독하고, 마스터키 기억부(313)에 기억되어 있는 마스터키 Mk를 판독한다.

역변환부(391f)는 판독한 하나의 서브그룹키 Gjk와, 판독한 하나의 마스터키 Mk에 대하여 소정의 연산을 실시하여 변형키를 생성한다.

여기에서 소정의 연산이란 변환부(291d)에서 이용되는 소정의 연산과 같은 연산이다.

역변환부(391f)는 생성한 변형키를 역변환부(321)로 출력한다.

(3) 역변환부(321)

역변환부(321)는 마스터키 기억부(313)에 기억되어 있는 마스터키 Mk를 판독하고, 상기 판독한 마스터키 Mk를 복호알고리즘 D_i의 키로 하여 판독한 암호화 고유키 Ji에 복호알고리즘 D_i을 실시하여 고유키 Ki를 생성하는 대신 역변환부(391f)로부터 변형키를 수취하고, 수취한 변형키를 복호알고리즘 D_i의 키로 하여 판독한 암호화 고유키 Ji에 복호알고리즘 D_i을 실시하여 고유키 Ki를 생성한다.

3.7.3 메모리카드 판독기(400f)

메모리카드 판독기(400f)는 메모리카드 판독기(400)와 비교하면, 추가로 서브그룹키 기억부(490f), 역변환부(491f)를 갖고 있는 점이 다르다. 여기에서 서브그룹키 기억부(490f), 역변환부(491f)는 각각 서브그룹키 기억부(390f), 역변환부 (391f)와 마찬가지이므로 설명을 생략한다. 또 메모리카드 판독기(400f)의 역변환부(421)는 메모리카드 기입기(300f)의 역변환부(321)와 마찬가지이며, 메모리카드 판독기(400f)의 그 밖의 구성요소에 대해서는 메모리카드 판독기(400)의 구성요소와 마찬가지이므로 설명을 생략한다.

3.7.4 디지털 저작물 보호시스템(100f)의 동작

디지털 저작물 보호시스템(100f)의 동작에 대하여 설명한다.

메모리카드(200f)가 메모리카드 기입기(300f)에 장착된 경우의 개요동작 및 메모리카드(200f)가 메모리카드 판독기(400f)에 장착된 경우의 개요동작에 대해서는 디지털 저작물 보호시스템(100)과 마찬가지이므로 설명을 생략한다.

다음으로 메모리카드(200f)가 메모리카드 기입기(300f)에 장착된 경우의 상세한 인증동작에 대하여 도 22를 이용하여 디지털 저작물 보호시스템(100)의 경우와의 상위점을 중심으로 설명한다.

단계 S150f에서 변환부(291f)는 서브그룹키 기억부(290f)에 기억되어 있는 하나의 서브그룹키 Gjk를 판독하고, 마스터키 기억부(210)에 기억되어 있는 마스터키 Mk를 판독하고, 판독한 하나의 서브그룹키 Gjk와,

판독한 하나의 마스터키 Mk 에 대하여 소정의 연산을 실시하여 변형키 Mk를 생성하고, 변환부(291f)는 생성한 변형키 Mk 를 변환부(230)로 출력한다.

단계 S130에 있어서 변환부(230)는 변형키 Mk를 암호알고리즘 E_i의 키로 하여 고유키 Ki에 암호알고리즘 E_i을 실시하여 암호화 고유키 E_i(Mk , Ki)를 생성한다.

단계 S151f에서 역변환부(391f)는 서브그룹키 기억부(390f)에 기억되어 있는 하나의 서브그룹키 Gjk를 판독하고, 마스터키 기억부(313)에 기억되어 있는 마스터키 Mk를 판독하고, 판독한 하나의 서브그룹키 Gjk와, 판독한 하나의 마스터키 Mk 에 대하여 소정의 연산을 실시하여 변형키 Mk 를 생성하고, 생성한 변형키 Mk 를 역변환부(321)로 출력한다.

단계 S132에 있어서, 역변환부(321)는 변형키를 복호알고리즘 D_i의 키로 하여 암호화 고유키 E_i(Mk , Ki)에 복호알고리즘 D_i을 실시하여 고유키 $K'_i=D_i$(Mk , E_i(Mk , Ki))을 생성한다.

또 메모리카드(200f)가 메모리카드 판독기(400f)에 장착된 경우의 상세한 인증동작에 대해서는 상기와 마찬가지이므로 설명을 생략한다.

3. 7. 5 정리

디지털 저작물 보호시스템(100d)과 마찬가지로 하나의 디지털 저작물 운용시스템을 복수의 단체가 운영하는 경우, 이들의 단체의 수만큼 다른 서브그룹키가 존재하고, 이들의 다른 서브그룹키가 각각 상기 복수의 단체에 할당되므로 각 단체는 독자적인 서비스 제공이 가능해진다.

또 메모리카드의 기억용량은 한정되어 있으므로 메모리카드에 기억할 수 있는 마스터키의 수에는 제한이 있는 경우가 많고, 마스터키와 서브그룹키의 조합에 의하여 이용할 수 있는 키의 수를 늘릴 수 있다는 효과가 있다.

또 디지털 저작물 보호시스템(100f)에서, 변환부(291f)에 대하여 변환처리를 하게 하지 않고, 변환부(230)에 대하여 미디어고유키 기록부(220)에 기억되어 있는 고유키를 변환시키는 제어부 및 역변환부(391f)에 대하여 역변환처리를 하게 하지 않고, 역변환부(321)에 대하여 미디어고유키 정보기록부(320)에 기억되어 있는 암호화 고유키를 역변환시키는 제어부를 설치함으로써 각 단체마다 서브그룹키를 할당한 후 추가로 하나의 디지털 저작물 운용시스템에 하나의 마스터키를 할당하고, 각 단체의 공통의 서비스를 제공할 수도 있다.

또 디지털 저작물 보호시스템(100f)에서는 마스터키 기억부(210)와 마스터키 기억부(313)에 같은 마스터키가 기억되어 있다고 하고 있지만, 공개키방식을 이용하여 다음과 같이 해도 된다.

디지털 저작물 보호시스템(100f)에서는 메모리카드(200f)의 마스터키 기억부 (210)는 비밀키로서의 마스터키를 기억하고 있다. 메모리카드(200f)는 또 변환부 (291f)에 의해 생성되는 변형키로부터 공개키를 생성하는 공개키 생성부를 갖는다. 생성한 공개키는 메모리카드 기입기(300f)에 미리 배포된다. 메모리카드 기입기 (300f)에서 암호부(360)는 상기 생성된 공개키를 이용하여 저작물을 암호화한다.

3. 8. 다른 디지털 저작물 보호시스템

본 발명에 관한 또 다른 실시예의 하나로서의 디지털 저작물 보호시스템 (100g)은 도 23에 도시된 메모리카드(200g), 메모리카드 기입기(300g), 도시하지 않는 메모리카드 판독기(400g)로 구성된다.

메모리카드(200g), 메모리카드 기입기(300g), 메모리카드 판독기(400g)는 각각 메모리카드(200), 메모리카드 기입기(300), 메모리카드 판독기(400)와 같은 구성이므로 이하에서는 상위점을 중심으로 하여 설명한다.

3. 8. 1 메모리카드(200g)

메모리카드(200g)는 메모리카드(200)와 비교하면 추가로 서브그룹키 기억부 (290g), 변환부(291g)를 갖고 있는 점이 다르다. 또 메모리카드(200g)의 그 밖의 구성요소에 대해서는 이하에 설명이 없는 한 메모리카드(200)의 구성요소와 마찬가지이며 설명을 생략한다.

(1) 서브그룹키 기억부(290g)

서브그룹키 기억부(290g)는 미리 하나의 서브그룹키 Gjk를 기억하고 있다. 서브그룹키 Gjk는 56비트의 비트열로 이루어진다.

서브그룹키는 서브그룹키 기억부(290d)의 서브그룹키와 같으므로 설명은 생략한다.

(2) 변환부(291g)

변환부(291g)는 서브그룹키 기억부(290g)에 기억되어 있는 하나의 서브그룹키 Gjk를 판독하고, 미디어고유키 기억부(220)에 기억되어 있는 고유키 Ki를 판독한다.

변환부(291g)는 판독한 하나의 서브그룹키 Gjk와, 판독한 하나의 고유키 Ki 에 대하여 소정의 연산을 실시하고, 변형키를 생성한다.

여기에서 소정의 연산이란 변환부(291d)에서 이용되는 소정의 연산과 같은 연산이다.

변환부(291g)는 생성한 변형키를 상호인증부(250)의 암호부(252)로 출력한다.

(3) 암호부(252)

암호부(252)는 미디어고유키 기억부(220)로부터 고유키 Ki를 판독하고, 상기 판독한 고유키 Ki를 암호알고리즘 E2의 키로 하여 수취한 난수 R_i에 암호알고리즘 E_i를 실시하여 암호화난수 S_i을 생성하는 대신 변

환부(291g)로부터 변형키를 수취하고, 상기 수취한 변형키를 암호알고리즘 E_i의 키로 하여 수취한 난수 R_i에 암호알고리즘 E_i를 실시하고 암호화난수 S_i를 생성한다.

3. 8. 2 메모리카드 기입기(300g)

메모리카드 기입기(300g)는 메모리카드 기입기(300)와 비교하면, 추가로 서브그룹키 기억부(390g), 역변환부(391g)를 갖고 있는 점이 다르다. 또 메모리카드 기입기(300g)의 그 밖의 구성요소에 대해서는 이하에 설명이 없는 한 메모리카드 기입기(300)의 구성요소와 마찬가지이며 설명을 생략한다.

(1) 서브그룹키 기억부(390g)

서브그룹키 기억부(390g)는 서브그룹키 기억부(290g)와 마찬가지로 미리 하나의 서브그룹키 G_{jk}를 기억하고 있다. 서브그룹키 G_{jk}는 56비트의 비트열로 이루어진다.

서브그룹키 G_{jk}에 대해서는 서브그룹키 기억부(290g)에 기억되어 있는 서브그룹키 G_{jk}와 같으므로 설명을 생략한다.

(2) 역변환부(391g)

역변환부(391g)는 서브그룹키 기억부(390g)에 기억되어 있는 하나의 서브그룹키 G_{jk}를 판독하고, 미디어고유키 기억부(323)에 기억되어 있는 고유키 K_i를 판독한다.

역변환부(391g)는 판독한 하나의 서브그룹키 G_{jk}와, 판독한 하나의 고유키 K_i에 대하여 소정의 연산을 실시하고, 변형키를 생성한다.

여기에서 소정의 연산이란 변환부(291d)에서 이용되는 소정의 연산과 같은 연산이다.

역변환부(391g)는 생성된 변형키를 복호부(333)로 출력한다.

(3) 복호부(333)

복호부(333)는 미디어고유키 기억부(323)로부터 고유키 K_i를 판독하고, 상기 판독한 고유키 K_i를 복호알고리즘 D_i의 키로 하여, 수취한 암호화난수 S_i에 복호알고리즘 D_i를 실시하여 난수 R_i를 생성하는 대신 역변환부(391g)로부터 변형키를 수취하고, 상기 수취한 변형키를 복호알고리즘 D_i의 키로 하여, 수취한 암호화난수 S_i에 복호알고리즘 D_i를 실시하고 난수 R_i를 생성한다.

3. 8. 3 메모리카드 판독기(400g)

메모리카드 판독기(400g)는 메모리카드 판독기(400)와 비교하면 추가로 서브그룹키 기억부(490g), 역변환부(491g)를 갖고 있는 점이 다르다. 여기에서 서브그룹키 기억부(490g), 역변환부(491g)는 각각 서브그룹키 기억부(390g), 역변환부 (391g)와 마찬가지이므로 설명을 생략한다. 또 메모리카드 판독기(400g)의 복호부 (433)는 메모리카드 기입기(300g)의 복호부(333)와 마찬가지이고, 메모리카드 판독기(400g)의 그 밖의 구성요소에 대해서는 메모리카드 판독기(400)의 구성요소와 마찬가지이므로 설명을 생략한다.

3. 8. 4 디지털 저작물 보호시스템(100g)의 동작

디지털 저작물 보호시스템(100g)의 동작에 대하여 설명한다.

메모리카드(200g)가 메모리카드 기입기(300g)에 장착된 경우의 개요동작 및 메모리카드(200g)가 메모리카드 판독기(400g)에 장착된 경우의 개요동작에 대해서는 디지털 저작물 보호시스템(100)과 마찬가지이므로 설명을 생략한다.

다음으로 메모리카드(200g)가 메모리카드 기입기(300g)에 장착된 경우의 상세한 인증동작에 대하여 도 24를 이용하여 디지털 저작물 보호시스템(100)의 경우와의 상위점을 중심으로 설명한다.

단계 S150g에서 변환부(291g)는 서브그룹키 기억부(290g)에 기억되어 있는 하나의 서브그룹키 G_{jk}를 판독하고, 미디어고유키 기억부(220)에 기억되어 있는 고유키 K_i를 판독하고, 판독한 하나의 서브그룹키 G_{jk}와, 판독한 하나의 고유키 K_i에 대하여 소정의 연산을 실시하고, 변형키를 생성하고, 생성한 변형키를 상호인증부 (250)의 암호부(252)로 출력한다.

단계 S135에서 암호부(252)는 변환부(291g)로부터 변형키를 수취하고, 상기 수취한 변형키를 암호알고리즘 E_i의 키로서, 수취한 난수 R_i에 암호알고리즘 E_i를 실시하여 암호화난수 S_i를 생성한다.

단계 S151g에서 역변환부(391g)는 서브그룹키 기억부(390g)에 기억되어 있는 하나의 서브그룹키 G_{jk}를 판독하고, 미디어고유키 기억부(323)에 기억되어 있는 고유키 K_i를 판독하고, 판독한 하나의 서브그룹키 G_{jk}와, 판독한 하나의 고유키 K_i에 대하여 소정의 연산을 실시하고, 변형키를 생성하고, 생성한 변형키를 복호부(333)로 출력한다.

단계 S137에서 복호부(333)는 역변환부(391g)로부터 변형키를 수취하고, 상기 수취한 변형키를 복호알고리즘 D_i의 키로서, 수취한 암호화난수 S_i에 복호알고리즘 D_i를 실시하고 난수 R_i를 생성한다.

또 메모리카드(200g)가 메모리카드 판독기(400g)에 장착된 경우의 상세한 인증동작에 대해서는 상기와 마찬가지이므로 설명을 생략한다.

3. 8. 5 정리

디지털 저작물 보호시스템(100d)과 마찬가지로 하나의 디지털 저작물 운용시스템을 복수의 단체가 운영하는 경우, 이들의 단체의 수만큼 다른 서브그룹키가 존재하며, 이들의 다른 서브그룹키가 각각 상기 복수의 단체에 할당되므로 각 단체는 독자적인 서비스의 제공이 가능해진다.

또 메모리카드의 기억용량은 한정되고 있으므로 메모리카드에 기억할 수 있는 마스터키의 수에는 제한이 있는 경우가 많고, 마스터키와 서브그룹키의 조합에 의하여 이용할 수 있는 키의 수를 늘릴 수 있다는 효과가 있다.

또 디지털 저작물 보호시스템(100g)에서 변환부(291g)에 대하여 변환처리를 하게 하지 않고, 변환부(230)에 대하여 미디어고유키 기록부(220)에 기억되어 있는 고유키를 변환시키는 제어부 및 역변환부(391g)에 대하여 역변환처리를 하게 하지 않고, 역변환부(321)에 대하여 미디어고유키 정보기록부(320)에 기억되어 있는 암호화 고유키를 역변환시키는 제어부를 설치함으로써 각 단체마다 서브그룹키를 할당한 후 추가로 하나의 디지털 저작물 운용시스템에 하나의 마스터키를 할당하고, 각 단체의 공통의 서비스를 제공할 수도 있다.

3.9 다른 디지털 저작물 보호시스템

본 발명에 관한 또 다른 실시예의 하나로서의 디지털 저작물 보호시스템 (100h)은 도 25 및 도 26에 도시된 메모리카드(200), 메모리카드 기입기(300h), 메모리카드 판독기(400h)로 구성된다.

메모리카드(200)는 디지털 저작물 보호시스템(100)의 메모리카드(200)와 동일하므로 설명을 생략한다. 또 메모리카드 기입기(300h), 메모리카드 판독기(400h)는 각각 메모리카드 기입기(300), 메모리카드 판독기(400)와 같은 구성이므로 이하에서는 상위점을 중심으로 하여 설명한다.

3.9.1 메모리카드 기입기(300h)

메모리카드 기입기(300h)는 메모리카드 기입기(300)와 비교하면, 추가로 변환부(392), 사용자키 입력부(393)를 갖고 있는 점이 다르다. 또 메모리카드 기입기 (300h)의 그 밖의 구성요소에 대해서는 이하에 설명이 없는 한 메모리카드 기입기 (300)의 구성요소와 마찬가지이며, 설명을 생략한다.

(1) 사용자키 입력부(393)

사용자키 입력부(393)는 키보드 등의 입력장치를 포함하며, 사용자로부터 해당 사용자만이 알고 있고, 사용자 고유의 패스워드인 사용자키의 입력을 접수한다.

사용자키는 각각의 사용자가 결정할 수 있고, 10자릿수 이내의 영숫자, 기호의 편성으로 이루어진다.

사용자키 입력부(393)는 사용자키의 입력을 접수하면 입력을 접수한 사용자키를 변환부(392)로 출력한다.

(2) 변환부(392)

변환부(392)는 미디어고유키 기억부(323)로부터 고유키 K_i를 판독하고, 사용자키 입력부(393)로부터 사용자키를 수취한다.

변환부(392)는 판독한 고유키 K_i와, 수취한 사용자키에 대하여 소정의 연산을 실시하고, 변형키를 생성한다. 여기에서 소정의 연산이란 배타적 논리합이다.

변환부(392)는 생성된 변형키를 암호부(360)로 출력한다.

(3) 암호부(360)

암호부(360)는 미디어고유키 기억부(323)로부터 고유키 K_i를 판독하고, 판독한 저작물을 복수의 64비트의 비트열로 이루어지는 부분저작물 $C_i(i=1, 2, 3, \cdots)$으로 분할하고, 상기 판독한 고유키 K_i를 암호알고리즘 E_1의 키로 하여, 각 부분저작물 $C_i(i=1, 2, 3, \cdots)$에 암호알고리즘 E_1를 실시하여 복수의 암호화 부분저작물 $F_i(i=1, 2, 3, \cdots)$를 생성하는 대신 변환부(392)로부터 변형키를 수취하고, 판독한 저작물을 복수의 64비트의 비트열로 이루어지는 부분저작물 $C_i(i=1, 2, 3, \cdots)$로 분할하고, 수취한 변형키를 암호알고리즘 E_2의 키로서, 각 부분저작물 $C_i(i=1, 2, 3, \cdots)$에 암호알고리즘 E_1를 실시하여 복수의 암호화 부분저작물 $F_i(i=1, 2, 3, \cdots)$를 생성한다.

3.9.2 메모리카드 판독기(400h)

메모리카드 판독기(400h)는 메모리카드 판독기(400)와 비교하면, 추가로 변환부(492), 사용자키 입력부(493)를 갖고 있는 점이 다르다. 또 메모리카드 판독기 (400h)의 그 밖의 구성요소에 대해서는 이하에 설명이 없는 한 메모리카드 판독기 (400)의 구성요소와 마찬가지이며 설명을 생략한다.

(1) 사용자키 입력부(493)

사용자키 입력부(493)는 사용자키 입력부(393)와 마찬가지로 사용자로부터 사용자키의 입력을 접수하고, 입력을 접수한 사용자키를 변환부(492)로 출력한다.

(2) 변환부(492)

변환부(492)는 변환부(392)와 마찬가지로 미디어고유키 기억부(423)로부터 고유키 K_i를 판독하고, 사용자키 입력부(493)로부터 사용자키를 수취하고, 판독한 고유키 K_i와, 수취한 사용자키에 대하여 소정의 연산을 실시하고, 변형키를 생성한다. 여기에서, 소정의 연산이란 배타적 논리합이다.

변환부(492)는 생성된 변형키를 복호부(460)로 출력한다.

(3) 복호부(460)

복호부(460)는 미디어고유키 기억부(423)로부터 고유키 K_i를 판독하고, 수취한 암호화저작물을 복수의 64비트의 비트열로 이루어지는 부분암호화저작물 $G_i(i=1, 2, 3, \cdots)$로 분할하고, 상기 판독한 고유키 K_i를 복호알고리즘 D_2의 키로서, 각 부분암호화저작물 $G_i(i=1, 2, 3, \cdots)$로 복호알고리즘 D_1를 실시

하여 복수의 부분저작물 $H_i(i=1, 2, 3, \cdots)$를 생성하는 대신에 변환부(492)로부터 변형키를 수취하고, 수취한 암호화저작물을 복수의 64비트의 비트열로 이루어지는 부분암호화저작물 $G_i(i=1, 2, 3, \cdots)$로 분할하고, 수취한 변형키를 복호알고리즘 D_2의 키로 하여, 각 부분암호화저작물 $G_i(i=1, 2, 3, \cdots)$로 복호알고리즘 D_2를 실시하여 복수의 부분저작물 $H_i(i=1, 2, 3, \cdots)$를 생성한다.

3. 9. 3 디지털 저작물 보호시스템(100h)의 동작

디지털 저작물 보호시스템(100)h의 동작에 대하여 설명한다.

메모리카드(200)가 메모리카드 기입기(300h)에 장착된 경우의 상세한 인증동작 및 메모리카드(200)가 메모리카드 판독기(400h)에 장착된 경우의 상세한 인증동작에 대해서는 디지털 저작물 보호시스템(100)과 동일하므로 설명을 생략하고, 메모리카드(200)가 메모리카드 기입기(300h)에 장착된 경우의 개요동작 및 메모리카드(200)가 메모리카드 판독기(400h)에 장착된 경우의 개요동작에 대하여 이하에 설명한다.

(1) 메모리카드(200)가 메모리카드 기입기(300h)에 장착된 경우의 개요동작

메모리카드(200)가 메모리카드 기입기(300h)에 장착된 경우의 개요동작에 대해서는 도 70에 도시된 흐름도의 단계 S114의 상세한 내용이 디지털 저작물 보호시스템(100)의 동작과 다를 뿐이므로 다음에 도 270에 도시된 흐름도를 이용하여 단계 S114의 상세한 내용에 대하여 설명한다.

사용자키 입력부(393)는 사용자로부터 사용자키의 입력을 접수하고, 입력을 접수한 사용자키를 변환부(392)로 출력하고(단계 S100h), 변환부(392)는 미디어고유키 기억부(323)로부터 고유키 K_i를 판독하고, 사용자키 입력부(393)로부터 사용자키를 수취하여 판독한 고유키 K_i와, 수취한 사용자키에 대하여 소정의 연산을 실시하고, 변형키를 생성하고, 생성한 변형키를 암호부(360)로 출력하고(단계 S101h), 암호부(360)는 변환부(392)로부터 변형키를 수취하고, 판독한 저작물을 복수의 64비트의 비트열로 이루어지는 부분저작물 $C_i(i=1, 2, 3, \cdots)$로 분할하고, 수취한 변형키를 암호알고리즘 E_2의 키로서, 각 부분저작물 $C_i(i=1, 2, 3, \cdots)$로 암호알고리즘 E_2를 실시하고 복수의 암호화 부분저작물 $F_i(i=1, 2, 3, \cdots)$를 생성하고, 생성한 암호화 부분저작물 F_i를 통신부(340)로 출력하고(단계 S102h), 통신부(340)는 암호화 부분저작물 F_i을 메모리카드(200)의 통신부(270)로 출력한다(단계 S103h).

(2) 메모리카드(200)가 메모리카드 판독기(400h)에 장착된 경우의 개요동작

메모리카드(200)가 메모리카드 판독기(400h)에 장착된 경우의 개요동작에 대해서는 도 80에 도시된 흐름도의 단계 S125의 상세한 내용이 디지털 저작물 보호시스템(100)의 동작과 다를 뿐이므로 다음에 도 280에 도시된 흐름도를 이용하여 단계 S125의 상세한 내용에 대하여 설명한다.

사용자키 입력부(493)는 사용자로부터 사용자키의 입력을 접수하고, 입력을 접수한 사용자키를 변환부(492)로 출력하고(단계 S111h), 변환부(492)는 미디어고유키 기억부(423)로부터 고유키 K_i를 판독하고, 사용자키 입력부(493)로부터 사용자키를 수취하고, 판독한 고유키 K_i와, 수취한 사용자키에 대하여 소정의 연산을 실시하고, 변형키를 생성하고, 생성한 변형키를 복호부(460)로 출력하고(단계 S112h), 복호부(460)는 변환부(492)로부터 변형키를 수취하고, 수취한 암호화저작물을 복수의 64비트의 비트열로 이루어지는 부분암호화저작물 $G_i(i=1, 2, 3, \cdots)$로 분할하고, 수취한 변형키를 복호알고리즘 D_2의 키로 하여, 각 부분암호화저작물 $G_i(i=1, 2, 3, \cdots)$에 복호알고리즘 D_2를 실시하고 복수의 부분저작물 $H_i(i=1, 2, 3, \cdots)$를 생성한다(단계 S113h).

3. 9. 5 정리

사용자는 자신이 설정한 사용자키를 이용하여 저작물을 암호화하고, 암호화한 저작물을 상기 사용자키를 이용하여 복호할 수 있으므로 사용자 자신의 저작물이 남에게 해독되지 않고, 보호할 수 있다고 하는 효과가 있다.

3. 10. 다른 디지털 저작물 보호시스템

본 발명에 관한 또 다른 실시예의 하나로서의 디지털 저작물 보호시스템 (100i)은 도 29 및 도 30에 도시된 메모리카드(200i), 메모리카드 기입기(300i), 메모리카드 판독기(400i)로 구성된다.

메모리카드(200i), 메모리카드 기입기(300i), 메모리카드 판독기(400i)는 각각 디지털 저작물 보호시스템(100)의 메모리카드(200), 메모리카드 기입기(300), 메모리카드 판독기(400)와 같은 구성이므로 이하에서는 상위점을 중심으로 하여 설명한다.

3. 10. 1 메모리카드 기입기(300i) 메모리카드 기입기(300i)는 메모리카드 기입기(300)와 비교하면 추가로 암호부(365), 파일키 생성부(366)를 갖고 있는 점이 다르다. 또 메모리카드 기입기(300i)의 그 밖의 구성요소에 대해서는 이하에 설명이 없는 한 메모리카드 기입기(300)의 구성요소와 마찬가지이며, 설명을 생략한다.

(1) 제어부(350)

제어부(350)는 저작물 취득부(380)에 대하여 파일마다 외부로부터의 저작물취득을 지시하는 저작물 취득신호를 출력하고, 또 파일키 생성부(366)에 대하여, 파일마다 파일키를 생성하는 생성지시를 출력한다.

(2) 저작물 취득부(380)

저작물 취득부(380)는 하나의 저작물을 파일로서 취득한다. 여기에서 파일이란 일정한 규칙으로 모은 데이터의 집합이다. 예를 들면 음악의 저작물인 경우는 1곡이 하나의 파일에 상당한다.

(3) 저작물 기억부(370)

저작물 기억부(370)는 파일마다 저작물을 기억한다.

(4) 파일키 생성부(366)

파일키 생성부(366)는 제어부(350)로부터의 생성지시를 받아 56비트로 이루어지는 파일키를 랜덤하게 생성하고, 생성한 파일키를 암호부(365)로 출력한다. 또 생성한 파일키를 암호부(360)로 출력한다.

또 파일키를 랜덤하게 생성한다고 하고 있지만, 파일키 생성부(366)는 조작자로부터 파일키의 입력을 수취한다고 해도 된다.

(5) 암호부(365)

암호부(365)는 미디어고유키 기억부(323)로부터 고유키 K_i를 판독하고, 파일키 생성부(366)로부터 파일키를 수취한다.

암호부(365)는 DES에 의해 규격되어 있는 암호알고리즘 E_s를 미리 기억하고 있다.

암호부(365)는 수취한 파일키에 암호알고리즘 E_s를 실시하여 암호화 파일키를 생성한다. 이 때 상기 판독한 고유키 K_i를 암호알고리즘 E_s의 키로 한다.

암호부(365)는 생성한 암호화 파일키를 통신부(340)로 출력한다.

(6) 암호부(360)

암호부(360)는 미디어고유키 기억부(323)로부터 고유키 K_i를 판독하고, 판독한 저작물을 복수의 64비트의 비트열로 이루어지는 부분저작물 C_i(i=1, 2, 3, ···)로 분할하고, 상기 판독한 고유키 K_i를 암호알고리즘 E_s의 키로 하여, 각 부분저작물 C_i(i=1, 2, 3, ···)에 암호알고리즘 E_s를 실시하고 복수의 암호화 부분저작물 F_i(i=1, 2, 3, ···)를 생성하는 대신 암호부(360)는 파일마다 저작물을 판독하고, 파일키 생성부(366)로부터 파일키를 수취하고, 파일마다 판독한 저작물을 복수의 64비트의 비트열로 이루어지는 부분저작물 C_i(i=1, 2, 3, ···)로 분할하고, 수취한 파일키를 암호알고리즘 E_s의 키로 하여, 각 부분저작물 C_i(i=1, 2, 3, ···)에 암호알고리즘 E_s를 실시하여 복수의 암호화 부분저작물 F_i(i=1, 2, 3, ···)를 생성한다.

(7)통신부(340)

통신부(340)는 추가로 암호부(365)로부터 암호화 파일키를 수취하고, 수취한 암호화 파일키를 통신부(270)로 출력한다.

3. 10. 2. 메모리카드(200i)

메모리카드(200i)에 대하여 메모리카드(200)와 비교하여 다른 구성요소에 관해서 그 상위점을 중심으로 이하에 설명한다.

(1) 통신부(270)

통신부(270)는 추가로 통신부(340)로부터 암호화 파일키를 수취하고, 수취한 암호화 파일키를 암호화저작물 기억부(260)로 출력한다.

또 통신부(270)는 추가로 암호화저작물 기억부(260)로부터 암호화 파일키 (261)를 판독하고, 판독한 암호화 파일키를 통신부(440)로 출력한다.

(2) 암호화저작물 기억부(260)

암호화저작물 기억부(260)는 추가로 통신부(270)로부터 암호화 파일키를 수취하고, 수취한 암호화 파일키(261)를 기억한다.

또 암호화저작물 기억부(260)는 통신부(270)로부터 수취한 암호화 부분저작물 F_i(i=1, 2, 3, ···)를 암호화파일(262)로서 기억한다.

3. 10. 3 메모리카드 판독기(400i)

메모리카드 판독기(400i)는 메모리카드 판독기(400)와 비교하면 추가로 복호부(465)를 갖고 있는 점이 다르다. 또 메모리카드 판독기(400i)의 그 밖의 구성요소에 대해서는 이하에 설명이 없는 한 메모리카드 판독기(400)의 구성요소와 마찬가지이며, 설명을 생략한다.

(1) 통신부(440)

통신부(440)는 추가로 통신부(270)로부터 암호화 파일키를 수취하고, 수취한 암호화 파일키를 복호부(465)로 출력한다.

(2) 복호부(465)

복호부(465)는 미디어고유키 기억부(423)로부터 고유키 K_i를 판독하고, 통신부(440)로부터 암호화 파일키를 수취한다.

복호부(465)는 DES에 의해 규격되어 있는 복호알고리즘 D_s를 미리 기억하고 있다.

여기에서 암호부(365)에 기억되어 있는 암호알고리즘 E_s와 복호알고리즘 D_s 사이에는, 다음의 수학식 17에 나타내는 관계가 있다.

$E_j = cr\,p.t\ (D_e)$

복호부(465)는 수취한 암호화 파일키에 복호알고리즘 D_e를 실시하여 파일키를 생성한다. 이 때 상기 판독한 고유키 K_i를 복호알고리즘 D_e의 키로 한다.

복호부(465)는 생성한 파일키를 복호부(460)로 출력한다.

(3) 복호부(460)

복호부(460)는 미디어고유키 기억부(423)로부터 고유키 K_i를 판독하고, 수취한 암호화저작물을 복수의 64비트의 비트열로 이루어지는 부분암호화저작물 $G_i(i=1, 2, 3, \cdots)$로 분할하고, 상기 판독한 고유키 K_i를 복호알고리즘 D_2의 키로서, 각 부분암호화저작물 $G_i(i=1, 2, 3, \cdots)$에 복호알고리즘 D_2를 실시하여 복수의 부분저작물 $H_i(i=1, 2, 3, \cdots)$를 생성하는 대신 복호부(465)로부터 파일키를 수취하고, 수취한 암호화저작물을 복수의 64비트의 비트열로 이루어지는 부분암호화저작물 $G_i(i=1, 2, 3, \cdots)$로 분할하여, 수취한 파일키를 복호알고리즘 D_e의 키로서, 각 부분암호화저작물 $G_i(i=1, 2, 3, \cdots)$에 복호알고리즘 D_e를 실시하여 복수의 부분저작물 $H_i(i=1, 2, 3, \cdots)$를 생성한다.

3. 10. 4 디지털 저작물 보호시스템(100i)의 동작

디지털 저작물 보호시스템(100i)의 동작에 대하여 설명한다.

메모리카드(200i)가 메모리카드 기입기(300i)에 장착된 경우의 상세한 인증동작 및 메모리카드(200i)가 메모리카드 판독기(400i)에 장착된 경우의 상세한 인증동작에 대해서는 디지털 저작물 보호시스템(100)과 동일하므로 설명을 생략하고, 메모리카드(200i)가 메모리카드 기입기(300i)에 장착된 경우의 개요동작 및 메모리카드(200i)가 메모리카드 판독기(400i)에 장착된 경우의 개요동작에 대하여 이하에 설명한다.

(1) 메모리카드(200i)가 메모리카드 기입기(300i)에 장착된 경우의 개요동작

메모리카드(200i)가 메모리카드 기입기(300i)에 장착된 경우의 개요동작에 대해서는 도 7에 도시된 흐름도의 단계 S114의 상세한 내용이 디지털 저작물 보호시스템(100)의 동작과 다를 뿐이므로, 다음에, 도 31에 도시된 흐름도를 이용하여 단계 S114의 상세한 내용에 대하여 설명한다.

파일키 생성부(366)는 제어부(350)로부터 생성지시를 받고, 64비트로 이루어지는 파일키를 랜덤하게 생성하고, 생성한 파일키를 암호부(365)로 출력하고, 암호부(365)는 미디어고유키 기억부(323)로부터 고유키 K_i를 판독하고, 파일키 생성부 (366)로부터 파일키를 수취하고, 상기 판독한 고유키 K_i를 암호알고리즘 E_s의 키로 하여, 암호부(365)는 수취한 파일키에 암호알고리즘 E_s를 실시하여 암호화 파일키를 생성하고, 생성한 암호화 파일키를 통신부(340)로 출력한다(단계 S100i). 통신부 (340)는 암호부(365)로부터 암호화 파일키를 수취하고, 수취한 암호화 파일키를 통신부(270)로 출력한다(단계 S101i). 암호부(360)는 파일키 생성부(366)로부터 파일키를 수취하고, 판독한 저작물을 복수의 64비트의 비트열로 이루어지는 부분저작물 $C_i(i=1, 2, 3, \cdots)$로 분할하고, 수취한 파일키를 암호알고리즘 E_e의 키로 하여, 각 부분저작물 $C_i(i=1, 2, 3, \cdots)$에 암호알고리즘 E_e를 실시하고 복수의 암호화 부분저작물 $F_i(i=1, 2, 3, \cdots)$를 생성한다(단계 S102i). 통신부(340)는 암호부 (360)로부터 복수의 암호화 부분저작물을 수취하고, 수취한 복수의 암호화 부분저작물을 통신부(270)로 출력한다(단계 S103i).

(2) 메모리카드(200i)가 메모리카드 판독기(400i)에 장착된 경우의 개요동작

메모리카드(200i)가 메모리카드 판독기(400i)에 장착된 경우의 개요동작에 대해서는 도 8에 도시된 흐름도의 단계 S125의 상세한 내용이 디지털 저작물 보호시스템(100)의 동작과 다를 뿐이므로 다음에 도 32에 도시된 흐름도를 이용하여 단계 S125의 상세한 내용에 대하여 설명한다.

통신부(440)는 통신부(270)로부터 암호화 파일키를 수취하고, 수취한 암호화 파일키를 복호부(465)로 출력하고, 복호부(465)는 미디어고유키 기억부(423)로부터 고유키 K_i를 판독하고, 통신부(440)로부터 암호화 파일키를 수취하고, 상기 판독한 고유키 K_i를 복호알고리즘 D_s의 키로 하여, 복호부(465)는 수취한 암호화 파일키에 복호알고리즘 D_s를 실시하여 파일키를 생성하고, 생성한 파일키를 복호부(460)로 출력한다(단계 S111i). 복호부(460)는 복호부(465)로부터 파일키를 수취하고, 수취한 암호화 저작물을 복수의 64비트의 비트열로 이루어지는 부분암호화저작물 $G_i(i=1, 2, 3, \cdots)$로 분할하고, 수취한 파일키를 복호알고리즘 D_e의 키로 하여, 각 부분암호화저작물 $G_i(i=1, 2, 3, \cdots)$에 복호알고리즘 D_e를 실시하고 복수의 부분저작물 $H_i(i=1, 2, 3, \cdots)$을 생성한다(단계 S112i).

3. 10. 5 정리

이상 설명한 바와 같이, 기록매체장치와 메모리카드 기입기인 액세스장치가 접속되고, 파일키를 이용하여 디지털 저작물을 암호화하여 기록매체장치에 기입하는 경우에 있어서, 기록매체장치와 액세스장치가 모두 정당성을 갖는다고 인증된 경우에 상기 액세스장치는 디지털 저작물을 구성하는 파일마다 파일키를 생성하고, 기록매체장치로부터 비밀전송된 고유키를 이용하여 1이상의 파일키를 암호화하여 각각 1이상의 암호화 파일키를 생성하며, 상기 디지털 저작물을 구성하는 파일마다 상기 파일키를 이용하여 파일을 암호화하여 암호화파일을 생성하고, 생성한 1이상의 상기 암호화 파일키와 1이상의 상기 암호화파일을 기록매체장치로 출력하고, 기록매체장치는 1이상의 상기 암호화 파일키와 1이상의 상기 암호화파일을 수취하여 기억한다.

또 1이상의 상기 암호화 파일키와 1이상의 상기 암호화파일을 기억하고 있는 기록매체장치와 메모리카드 판독기인 액세스장치가 접속되고 암호화파일을 복호하여 재생하는 경우에 있어서, 기록매체장치와 액세스

장치가 모두 정당성을 갖는다고 인증된 경우에 상기 기록매체장치는 1이상의 상기 암호화 파일키와 1이상의 상기 암호화파일을 상기 액세스장치로 출력하고, 상기 액세스장치는 상기 기록매체장치로부터 1이상의 상기 암호화 파일키와 1이상의 상기 암호화파일을 수취하고, 상기 암호화파일마다 기록매체장치로부터 비밀전송된 고유키를 이용하여 암호화 파일키를 복호하여 파일키를 생성하고, 생성한 파일키를 이용하여 상기 암호화파일을 복호하여 파일을 생성하고 생성한 파일을 재생한다.

이와 같이 하여 저작물을 형성하는 파일마다 다른 파일키를 생성하고, 생성된 다른 파일키로 파일단위의 저작물을 암호화하므로 파일이 도청되기 어렵게 되어 파일의 안전성이 향상된다는 효과가 있다.

또 디지털 저작물 보호시스템(100i)은 다음과 같이 구성해도 된다.

(1) 디지털 저작물 보호시스템(100i)의 변형예 1

디지털 저작물 보호시스템(100i)의 변형예를 도 33의 블록도에 도시한다.

도 33에 도시된 바와 같이 메모리카드(200i)는 추가로 난수 시드생성부(292)를 갖고, 난수 시드생성부(292)는 난수의 초기값인 시드를 생성한다. 여기에서 시드는 64비트로 이루어지는 시각이다. 시드는 시각 등의 값과 같이 시시각각 변화하는 값이 바람직하다. 난수시드 생성부(292)는 생성된 시드를 통신부(270)로 출력하고, 통신부(270)는 시드를 수취하고, 수취한 시드를 통신부(340)로 출력한다. 통신부(340)는 시드를 수취하고, 수취한 시드를 파일키 생성부(366)로 출력한다. 파일키 생성부(366)는 시드를 수취하고, 수취한 시드를 이용하여 난수를 발생시켜 발생시킨 난수를 파일키로 한다.

또 파일키 생성부(366)는 다음과 같이 하여 난수를 발생시킨다고 해도 된다.

파일키 생성부(366)는 상기 수취한 시드를 소정의 암호알고리즘을 이용하여 암호화하여 암호문을 생성한다. 여기에서 키는 소정의 키를 이용한다. 또 파일키 생성부(366)는 생성된 암호문을 상기 소정의 암호알고리즘을 이용하여 다시 암호화하여 암호문을 생성한다. 이 암호처리를 특정횟수 반복하고, 마지막으로 생성된 암호문을 상기 난수로 한다.

(2) 디지털 저작물 보호시스템(100i)의 변형예 2

디지털 저작물 보호시스템(100i)의 또 다른 변형예를 도 34의 블록도에 도시한다.

도 34에 도시된 바와 같이 메모리카드(200i)는 추가로 난수시드 생성부(293)를 갖고, 난수시드 생성부(293)는 난수시드 생성부(292)와 마찬가지로 난수의 초기값인 시드를 생성한다. 여기에서 시드는 64비트로 이루어지는 시각이다. 시드는 시각 등의 값과 같이 시시각각 변화하는 값이 바람직하다. 난수 시드생성부(293)는 생성된 시드를 상호인증부(250)로 출력한다. 상호인증부(250)는 상기 시드를 수취하고, 수취한 시드를 인증공정에 의해 통신부(270), 통신부(340)를 경유하여 상호인증부(330)로 출력한다. 상호인증부(330)는 시드를 수취하고, 수취한 시드를 파일키 생성부(366)로 출력한다. 파일키 생성부(366)는 시드를 수취하고, 수취한 시드를 이용하여 난수를 발생시켜 발생시킨 난수를 파일키로 한다.

다음으로 상기 인증공정의 동작의 상세한 내용에 대하여 도 9 및 도 10에 도시된 흐름도와의 상위점을 중심으로 설명한다.

단계 S135에서 암호부(252)는 난수 시드생성부(293)로부터 시드 S를 수취하고, 난수 R_i과 시드 S를 결합하고, (R_i + S)를 생성하여 합계 128비트의 비트열로 한다. 암호부(252)는 고유키 Ki를 암호알고리즘 E_2의 키로 하여, (R1 + S)에 암호알고리즘 E_2를 실시하여 암호화난수 $E_2(Ki, (R_i + S))$를 생성한다. 여기에서, (R_i + S)는 128비트의 비트열이므로 64비트씩의 2블록으로 나누어 암호화한다.

단계 S136에서 통신부(270)는 통신부(340)를 경유하여 2블록의 암호화난수 $E_2(Ki, (R_i + S))$를 복호부(333)로 출력한다.

단계 S137에 있어서, 복호부(333)는 고유키 K i를 복호알고리즘 D_2의 키로 하여, 암호화난수 $E_2(Ki, (R_i + S))$에 복호알고리즘 D_2를 실시하고, $D_2(K i, E_2(Ki, (R_i + S)))$를 생성한다. 복호부(333)는 $D_2(K i, E_2(Ki, (R_i + S)))$를 전반의 64비트의 비트열과 후반의 64비트의 비트열로 분리한다.

단계 S138에서 상호인증 제어부(334)는 난수 R_i과 상기 전반 64비트의 비트열을 비교하여 일치하고 있으면 메모리카드(200)는 정당한 장치라고 인식하고, 일치하지 않으면, 메모리카드(200)는 부정한 장치라고 인식한다. 또 일치하고 있는 경우에는 상호인증 제어부(334)는 후반의 64비트의 비트열이 시드 S라고 판단하여, 시드 S를 파일키 생성부(366)로 출력한다.

또 상기에 있어서, 난수 R_i과 시드 S를 결합하여 (R_i + S)를 생성한다고 하고 있지만, 난수 R_i을 32비트씩의 전반비트열과 후반비트열로 분리하고, 시드 S를 32비트씩의 전반비트열과 후반비트열로 분리하고, 난수 R_i의 전반비트열과, 시드 S의 전반비트열과, 난수 R_i의 후반비트열, 시드 S의 후반비트열을 이 순서로 결합한다고 해도 된다.

(3) 디지털 저작물 보호시스템(100i)의 변형예 3

상기 저작물이 어떤 논리적 혹은 물리적 단위마다 1개 이상의 데이터블록으로 구성되어 있는 것으로 하고, 상기 저작물의 각 데이터블록을 암호화하여 기록매체에 전송하고, 혹은 기록매체로부터 전송된 저작물을 복호할 때 각 데이터블록 고유의 데이터블록키를 생성하고, 상기 기기인증을 거쳐 얻은 고유키와, 데이터블록키를 이용하여, 대응하는 데이터블록을 암호화하여, 기록매체에 전송하고 혹은 기록매체로부터 전송된 데이터블록을 복호하도록 해도 된다.

보다 구체적으로는 메모리카드(200i)와 메모리카드 기입기(300i)가 모두 정당성을 갖는다고 인증된 경우에, 메모리카드 기입기(300i)는 상기 저작물을 분할하여 1이상의 데이터블록을 생성하고, 생성한 상기 데

이터블록마다 데이터블록키를 생성하고, 상기 고유키와 상기 데이터블록에 대응하는 상기 데이터블록키를 이용하여 상기 데이터블록을 암호화하여 암호화 데이터블록을 생성하고, 생성한 암호화 데이터블록을 메모리카드(200i)로 전송한다고 해도 된다. 또 메모리카드(200i)와 메모리카드 판독기(400i)가 모두 정당성을 갖는다고 인증된 경우에 메모리카드 판독기(400i)는 메모리카드(200i)로부터 암호화된 저작물을 구성하는 1이상의 암호화데이터블록을 수신하고, 수신한 상기 암호화 데이터블록마다 데이터블록키를 생성하고, 상기 고유키와 상기 암호화 데이터블록에 대응하는 상기 데이터블록키를 이용하여 수신한 상기 암호화 데이터블록을 복호하여 데이터블록을 생성하도록 해도 된다.

이 구성에 의하면 저작물을 형성하는 데이터블록마다 다른 데이터블록키를 생성하여 생성된 다른 데이터블록키로 데이터블록단위의 저작물을 암호화하기 때문에 데이터블록이 도청되기 어렵게 되어 데이터블록의 안전성이 향상된다는 효과가 있다.

3. 1.1 다른 디지털 저작물 보호시스템

본 발명에 관한 또 다른 실시예의 하나로서의 디지털 저작물 보호시스템 (100j)은 도시하지 않는 메모리카드(200j), 메모리카드 기입기(300j), 메모리카드 판독기(400j)로 구성된다.

메모리카드(200j)는 메모리카드(200j)가 기억하고 있는 고유키를 메모리카드 기입기(300j)로 비밀전송하고, 메모리카드 기입기(300j)는 비밀전송된 고유키를 이용하여 메모리카드(200j)의 정당성을 인증하고, 다음으로 메모리카드(200j)는 고유키를 이용하여 메모리카드 기입기(300j)의 정당성을 인증하여, 서로 정당성을 인증할 수 있었던 경우에 메모리카드 기입기(300j)는 디지털 저작물을 메모리카드 (200j)로 출력한다. 메모리카드(200j)와 메모리카드 판독기(400j) 사이에 있더라도 마찬가지로 하여 상대의 인증을 행한다.

메모리카드(200j), 메모리카드 기입기(300j), 메모리카드 판독기(400j)는 각각 디지털 저작물 보호시스템(100)의 메모리카드(200), 메모리카드 기입기(300), 메모리카드 판독기(400)와 같은 구성이므로 이하에서는 상위점을 중심으로 하여 설명한다.

3. 1.1. 1 메모리카드(200j)

메모리카드(200j)는 마스터키 기억부(210), 미디어고유키 기억부(220), 변환부(230), 미디어고유키 정보기억부(240), 상호인증부(250), 암호화저작물 기억부 (260), 통신부(270), 제어부(280)로 구성되고, 상호인증부(250)는 난수발생부 (251), 변환부(255), 상호인증 제어부(254)로 구성된다.

마스터키 기억부(210), 미디어고유키 기억부(220), 변환부(230), 미디어고유키 정보기억부(240)는 각각 메모리카드(200)의 같은 부호를 갖는 구성요소와 동일하므로 다른 구성요소에 대하여 설명한다.

(1) 난수발생부(251)

난수발생부(251)는 난수 R_2를 생성한다. 난수 R_2는 64비트의 비트열로 이루어진다. 난수발생부(251)는 생성된 난수 R_2를 통신부(270)와 변환부(255)에 출력한다.

(2) 변환부(255)

변환부(255)는 함수 f_i을 미리 기억하고 있다.

변환부(255)는 통신부(270)로부터 난수 R_i을 수취하고, 미디어고유키 기억부 (220)로부터 고유키 Ki를 판독하고, 수취한 난수 R_i에 고유키 Ki를 이용하여 함수 f_i을 실시하여 변환계수 Q_i을 생성한다. 생성된 변환계수 Q_i은 다음의 수학식 18에 나타낸 바와 같이 표현할 수 있다.

$$Q_i = f_i(Ki, R_i)$$

여기에서 f_i은 일방향성 함수이다. 일방향성 함수란 입력값으로부터 출력값으로의 방향의 계산은 간단하지만, 역방향인 출력값으로부터 입력값으로의 계산이 곤란한 성질을 갖는 함수를 말한다. 일방향성 함수의 일례는 암호화 함수이다.

변환부(255)는 생성된 변환계수 Q_i을 통신부(270)로 출력한다.

또 변환부(255)는 난수발생부(251)로부터 난수 R_2를 수취하고, 미디어고유키 기억부(220)로부터 고유키 Ki를 판독하고, 고유키 Ki를 이용하여 수취한 난수 R_2에 함수 f_i을 실시하여 변환계수 Q_i를 생성한다. 생성된 변환계수 Q_i는 다음의 수학식 19에 나타낸 바와 같이 표현할 수 있다.

$$Q_i = f_i(Ki, R_2)$$

변환부(255)는 생성한 변환계수 Q_i를 상호인증 제어부(254)로 출력한다.

(3)상호인증 제어부(254)

상호인증 제어부(254)는 변환부(255)로부터 변환계수 Q_i를 수취하고; 또 통신부(270)로부터 변환계수 Q'_i를 수취한다.

상호인증 제어부(254)는 변환계수 Q_i와 변환계수 Q'_i를 비교하여, 일치하면 메모리카드(200j)가 장착된 메모리카드 기입기(300j) 또는 메모리카드 판독기 (400j)가 정당한 장치라고 인증하고, 일치하지 않으면

메모리카드(200j)가 장착된 메모리카드 기입기(300j) 또는 메모리카드 판독기(400j)가 부정한 장치라고 간주한다.

상호인증 제어부(254)는 메모리카드 기입기(300j) 또는 메모리카드 판독기 (400j)가 정당한 장치인지 부정한 장치인지를 나타내는 인증신호를 제어부(280)로 출력한다.

(4) 통신부(270)

통신부(270)는 미디어고유키 정보기억부(240)로부터 암호화 고유키 J_i를 판독하고, 판독한 암호화 고유키 J_i를 메모리카드 기입기(300j)의 통신부(340) 또는 메모리카드 판독기(400j)의 통신부(440)로 출력한다.

통신부(270)는 메모리카드 기입기(300j)의 통신부(340)로부터 또는 메모리카드 판독기(400j)의 통신부(440)로부터 난수 R_i을 수취하고, 수취한 난수 R_i을 상호인증부(250)의 변환부(255)로 출력한다.

통신부(270)는 변환부(255)로부터 변환계수 Q_i을 수취하고, 수취한 변환계수 Q_i을 메모리카드 기입기(300j)의 통신부(340) 또는 메모리카드 판독기(400j)의 통신부(440)로 출력한다.

통신부(270)는 난수발생부(251)로부터 난수 R_2를 수취하고, 수취한 난수 R_2를 메모리카드 기입기(300j)의 통신부(340) 또는 메모리카드 판독기(400j)의 통신부 (440)로 출력한다.

통신부(270)는 메모리카드 기입기(300j)의 통신부(340) 또는 메모리카드 판독기(400j)의 통신부(440)로부터 변환계수 Q_2를 수취하고, 수취한 변환계수 Q_2를 상호인증부(250)의 상호인증 제어부(254)로 출력한다.

또, 통신부(270)는 메모리카드(200)의 통신부(270)와 마찬가지로 제어부(280)로부터 통신중지신호를 수취하면 메모리카드 기입기(300j)의 통신부(340) 또는 메모리카드 판독기(400j)의 통신부(440)와의 통신을 중지한다. 또 메모리카드 기입기 (300j)의 통신부(340)로부터 암호화 부분저작물 F_i(i=1, 2, 3, ...)를 수취하고, 수취한 암호화 부분저작물 F_i(i=1, 2, 3, ...)를 암호화저작물 기억부(260)로 출력한다. 또 암호화저작물 기억부(260)로부터 암호화저작물을 판독하고, 판독한 암호화저작물을 메모리카드 판독기(400j)의 통신부(440)로 출력한다.

3. 11. 2 메모리카드 기입기(300j)

메모리카드 기입기(300j)는 마스터키 기억부(313), 미디어고유키 정보기억부 (320), 역변환부(321), 미디어고유키 기억부(323), 상호인증부(330), 통신부(340), 제어부(350), 암호부(360), 저작물 기억부(370), 저작물 취득부(380)로 구성되며, 저작물 취득부(380)는 통신회선(10)을 경유하여 외부와 접속되고, 상호인증부(330)는 난수발생부(331), 변환부(335), 상호인증 제어부(334)로 구성된다.

마스터키 기억부(313), 미디어고유키 정보기억부(320), 역변환부(321), 미디어고유키 기억부(323), 제어부(350), 암호부(360), 저작물 기억부(370), 저작물 취득부(380)는 각각 메모리카드 기입기(300)의 같은 부호를 갖는 구성요소와 동일하므로 다른 구성요소에 대하여 이하에 설명한다.

(1) 난수발생부(331)

난수발생부(331)는 난수 R_i을 생성한다. 난수 R_i은 64비트의 비트열로 이루어진다. 난수발생부(331)는 생성한 난수 R_i을 통신부(340)로 출력한다. 또 난수발생부 (331)는 생성한 난수 R_i을 변환부(335)로 출력한다.

(2) 변환부(335)

변환부(335)는 함수 f_i을 미리 기억하고 있다. 변환부(335)가 기억하고 있는 함수 f_i은 변환부(255)가 기억하고 있는 함수 f_i과 동일하다.

변환부(335)는 통신부(340)로부터 난수 R_2를 수취하고, 미디어고유키 기억부 (323)로부터 고유키 K_i를 판독하고, 고유키 K_i를 이용하여 수취한 난수 R_2에 함수 f_i을 실시하여 변환계수 Q_2를 생성한다. 생성된 변환계수 Q_2는 다음의 수학식 20에 나타낸 바와 같이 표현할 수 있다.

$$Q'_2 = f_i(K_i, R_2)$$

변환부(335)는 생성한 변환계수 Q'_2를 통신부(340)로 출력한다.

또, 변환부(335)는 난수발생부(331)로부터 난수 R_i을 수취하고, 미디어고유키 기억부(323)로부터 고유키 K_i를 판독하고, 고유키를 이용하여 수취한 난수 R_i에 함수 f_i을 실시하여 변환계수 Q'_i을 생성한다. 생성된 변환계수 Q'_i은 다음의 수학식 21에 나타낸 바와 같이 표현할 수 있다.

$$Q'_i = f_i(K_i, R_i)$$

변환부(335)는 생성된 변환계수 Q'_i를 상호인증 제어부(334)로 출력한다.

(3) 상호인증 제어부(334)

상호인증 제어부(334)는 변환부(335)로부터 변환계수 Q'_i을 수취하고, 통신부(340)로부터 변환계수 Q_i을

수취한다.

상호인증 제어부(334)는 변환계수 Q'_i과 변환계수 Q_i를 비교하여 일치하면 메모리카드 기입기(300j)에 장착된 메모리카드(200j)가 정당한 장치라고 인증하고, 일치하지 않으면 메모리카드 기입기(300j)에 장착된 메모리카드(200j)가 부정한 장치라고 간주한다.

상호인증 제어부(334)는 메모리카드 기입기(300j)에 장착된 메모리카드(200j)가 정당한 장치인지 부정한 장치인지를 나타내는 인증신호를 제어부(350)로 출력한다.

(4) 통신부(340)

통신부(340)는 메모리카드(200j)의 통신부(270)로부터 암호화 고유키 Ji를 수취하고, 수취한 암호화 고유키 Ji를 미디어고유키 정보기억부(320)로 출력한다.

통신부(340)는 난수발생부(331)로부터 난수 R_i을 수취하고, 수취한 난수 R_i을 메모리카드(200j)의 통신부(270)로 출력한다.

통신부(340)는 메모리카드(200j)의 통신부(270)로부터 변환계수 Q_i을 수취하고, 수취한 변환계수 Q_i를 상호인증부(330)의 상호인증 제어부(334)로 출력한다.

통신부(340)는 메모리카드(200j)의 통신부(270)로부터 난수 R_i를 수취하고, 수취한 난수 R_i를 상호인증부(330)의 변환부(335)로 출력한다.

통신부(340)는 변환부(335)로부터 변환계수 Q'_i를 수취하고, 수취한 변환계수 Q'_i를 메모리카드(200j)의 통신부(270)로 출력한다.

또, 통신부(340)는 메모리카드 기입기(300)의 통신부(340)와 같이, 제어부 (350)로부터 통신중지신호를 수취하면 메모리카드(200)의 통신부(270)와의 통신을 중지한다. 또한 암호부(360)로부터 암호화 부분저작물 F_i(i=1, 2, 3, ···)를 수취하고, 수취한 암호화 부분저작물 F_i(i=1, 2, 3, ···)를 메모리카드(200j)의 통신부(270)로 출력한다.

3. 1.1. 3 메모리카드 판독기(400j)

메모리카드 판독기(400j)는 마스터키 기억부(413), 미디어고유키 정보기억부 (420), 역변환부(421), 미디어고유키 기억부(423), 상호인증부(430), 통신부(440), 제어부(450), 복호부(460), 저작물 기억부(470), 재생부(480), 조작부 (490)로 구성되고, 상호인증부(430)는 난수발생부(431), 변환부(435), 상호인증 제어부(434)로 구성된다.

마스터키 기억부(413), 미디어고유키 정보기억부(420), 역변환부(421), 미디어고유키 기억부(423), 제어부(450), 복호부(460), 저작물 기억부(470), 재생부 (480), 조작부(490)는 각각 메모리카드 판독기(400)의 같은 부호를 붙인 구성요소와 동일하고, 또 통신부(440), 난수발생부(431), 변환부(435), 상호인증 제어부 (434)는 메모리카드 기입기(300j)의 통신부(340), 난수발생부(331), 변환부(335), 상호인증 제어부(334)와 마찬가지이므로 설명을 생략한다.

3. 1.1. 4 디지털 저작물 보호시스템(100j)의 동작

디지털 저작물 보호시스템(100j)의 동작에 대하여 설명한다.

메모리카드(200j)가 메모리카드 기입기(300j)에 장착된 경우의 개요동작 및 메모리카드(200j)가 메모리카드 판독기(400j)에 장착된 경우의 개요동작에 대해서는 디지털 저작물 보호시스템(100)과 동일하므로 설명을 생략하고, 메모리카드 (200j)가 메모리카드 기입기(300j)에 장착된 경우의 인증의 상세 동작에 대하여 이하에 설명한다. 또 메모리카드(200j)가 메모리카드 판독기(400j)에 장착된 경우의 인증의 상세한 동작은 메모리카드(200j)가 메모리카드 기입기(300j)에 장착된 경우의 인증의 상세 동작과 마찬가지이므로 설명을 생략한다.

(1) 메모리카드(200j)가 메모리카드 기입기(300j)에 장착된 경우의 인증의 상세한 동작

메모리카드(200j)가 메모리카드 기입기(300j)에 장착된 경우의 인증의 상세한 동작에 대하여 도 35를 이용하여 설명한다.

이 도면의 단계 S130~S134는 도 9의 단계 S130~S134와 동일하므로 설명을 생략한다.

변환부(335)는 난수발생부(331)로부터 난수 R_i을 수취하고, 미디어고유키 기억부(323)로부터 고유키 K i를 판독하고, 고유키를 이용하여 수취한 난수 R_i에 함수 f_i을 실시하여 변환계수 Q_i을 생성하여, 생성한 변환계수 Q'_i을 상호인증 제어부 (334)로 출력한다(단계 S162).

변환부(255)는 통신부(270)로부터 난수 R_i을 수취하고, 미디어고유키 기억부 (220)로부터 고유키 Ki를 판독하고, 수취한 난수 R_i에 고유키 Ki를 이용하여 함수 f_i을 실시하여 변환계수 Q_i을 생성하고(단계 S161), 생성한 변환계수 Q_i을 통신부 (270), 통신부(340)를 통해 상호인증 제어부(334)로 출력한다(단계 S163).

상호인증 제어부(334)는 변환계수 Q'_i과 변환계수 Q_i을 비교하여, 일치하면 메모리카드 기입기(300j)에 장착된 메모리카드(200j)가 정당한 장치라고 인증하고, 일치하지 않으면 메모리카드 기입기(300j)에 장착된 메모리카드(200j)가 부정한 장치라고 간주한다(단계 S164).

난수발생부(251)는 난수 R_i를 생성하고(단계 S165), 생성한 난수 R_i를 통신부 (270) 및 통신부(340)를 통해 변환부(335)로 출력한다(단계 S166).

변환부(335)는 통신부(340)로부터 난수 R를 수취하고, 미디어고유키 기억부 (323)로부터 고유키 K i를 판독하고, 고유키 K i를 이용하여 수취한 난수 R에 함수 f_1을 실시하고 변환계수 Q i를 생성한다(단계 S168).

변환부(335)는 생성한 변환계수 Q i를 통신부(340) 및 통신부(270)를 통해 상호인증 제어부(254)로 출력한다(단계 S169).

변환부(255)는 난수발생부(251)로부터 난수 R를 수취하고, 미디어고유키 기억부(220)로부터 고유키 Ki를 판독하고, 고유키 Ki를 이용하여 수취한 난수 R에 함수 f_1을 실시하여 변환계수 Q i를 생성한다(단계 S167).

상호인증 제어부(254)는 변환계수 Q i와 변환계수 Q i를 비교하여, 일치하면 메모리카드(200j)가 장착된 메모리카드 기입기(300j) 또는 메모리카드 판독기 (400j)가 정당한 장치라고 인증하고, 일치하지 않으면 메모리카드(200j)가 장착된 메모리카드 기입기(300j) 또는 메모리카드 판독기(400j)가 부정한 장치라고 간주한다 (단계 S170).

3. 11. 5 정리

이상 설명한 바와 같이, 디지털 저작물 보호시스템(100j)에 의하면 디지털 저작물 보호시스템(100)과 마찬가지로 정당한 장치로부터 부정한 장치로 저작물이 전송되는 것을 방지할 수 있으므로 정당하게 취득된 저작물이 부정히 이용되는 것을 방지할 수 있는 것과 아울러, 또 부정한 장치로부터 정당한 장치로 저작물이 전송되는 것을 방지할 수 있으므로 부정하게 취득된 저작물의 한층 더 이용을 방지할 수 있다.

또 기록매체장치는 소유하는 고유키를 마스터키를 이용하여 액세스장치에 비밀전송하고, 액세스장치는 비밀전송된 상기 고유키를 마스터키를 이용하여 복호한다. 액세스장치는 난수로서 생성한 인증정보를 기록매체장치에 전송하고, 상기 고유키를 이용하여 상기 인증정보에 함수를 실시한다. 기록매체장치는 상기 고유키를 이용하여 상기 인증정보에 같은 함수를 실시하여 액세스장치에 전송한다. 액세스장치는 기록매체장치로부터 수취한 함수가 실시된 인증정보와, 스스로 함수를 실시한 인증정보를 비교하여 일치하는 경우에 기록매체장치가 정당성을 갖는다고 인증하고, 일치하지 않는 경우에 기록매체장치가 정당성을 갖지 않는다고 인증한다. 또 기록 매체장치가 액세스장치를 인증하는 경우도 마찬가지이다. 이와 같이 구성되어 있으므로 장치는 접속된 상대의 장치가 정당한 장치인지 부정한 장치인지를 인증할 수 있다.

또 액세스장치 및 기록매체장치는 기록매체장치가 기억하고 있는 고유키를 이용하여 서로 상대의 장치를 인증하고, 디지털 저작물 보호시스템(100)과 같이 액세스장치가 기억하고 있는 장치키를 이용하지 않으므로 액세스장치 및 기록매체장치는 장치키 및 장치키정보를 기억하는 메모리, 장치키로부터 장치키정보로 변환하는 변환부 또는 역변환을 하는 역변환부를 필요로 하지 않고, 각각의 회로규모를 작게 할 수 있다.

3. 12 그 밖의 변형예

(1) 상기 실시예에서는 디지털 저작물 보호시스템은 메모리카드와 메모리카드 기입기와 메모리카드 판독기로 구성된다고 하고 있지만, 디지털 저작물 보호시스템은 메모리카드와 메모리카드 기입기로 구성된다고 해도 된다. 또 디지털 저작물 보호시스템은 메모리카드와 메모리카드 판독기로 구성된다고 해도 된다.

(2) 상기 실시예에서는 메모리카드를 일례로 하는 기록매체장치와 메모리카드 기입기 또는 메모리카드 판독기를 일례로 하는 액세스장치가 접속된 경우에, 서로 상대의 장치가 정당한 장치인지 부정한 장치인지를 인증하고, 서로 정당한 장치라고 인증된 경우에만 기록매체장치로부터 액세스장치로 저작물을 전송하고, 또 액세스장치로부터 기록매체장치로 저작물을 전송한다고 하고 있지만, 다음과 같이 해도 된다.

메모리카드 기입기를 일례로 하는 액세스장치로부터 메모리카드를 일례로 하는 기록매체장치로 저작물을 전송하는 경우에, 상기 기록매체장치와 상기 액세스장치가 접속된 경우에 상기 액세스장치가 상기 기록매체장치의 정당, 부정을 인증하여 상기 기록매체장치가 정당한 장치라고 인증된 경우에만 액세스장치로부터 기록매체장치로 저작물을 전송한다고 해도 된다. 이 경우에 상기 기록매체장치는 상기 액세스장치의 정당, 부정의 인증은 하지 않는다.

또 반대로 메모리카드를 일례로 하는 기록매체장치로부터 메모리카드 판독기를 일례로 하는 액세스장치로 저작물을 전송하는 경우에 상기 기록매체장치와 상기 액세스장치가 접속된 경우에 상기 기록매체장치가 상기 액세스장치의 정당, 부정을 인증하고, 상기 액세스장치가 정당한 장치라고 인증된 경우에만 기록매체장치로부터 액세스장치로 저작물을 전송한다고 해도 된다. 이 경우에 상기 액세스장치는 상기 기록매체장치의 정당, 부정의 인증은 하지 않는다.

이것은 저작물의 전송원의 장치가 전송장소의 장치의 정당, 부정을 인증함으로써 정당하게 취득된 저작물이 부정하게 이용되는 것을 방지한다는 사고방식에 근거하는 것이다.

(3) 상기 실시예에서는 액세스장치는 메모리카드 기입기 또는 메모리카드 판독기라고 하고 있지만, 액세스장치는 메모리카드 기입기 및 메모리카드 판독기의 양쪽의 구성을 겸비하고 있다고 해도 된다.

구체적으로는 도 2에 도시된 퍼스널 컴퓨터(500)에 메모리카드 기입기 및 메모리카드 판독기의 양쪽 구성을 겸비하고 있는 액세스장치가 접속되고, 메모리카드가 액세스장치에 삽입되어 접속된다. 이용자는 퍼스널 컴퓨터(500)를 이용하고, 외부로부터 통신회선(10)을 통해 음악 등의 저작물을 취득하고, 상기 액세스장치에 의해 취득한 저작물을 메모리카드에 기입한다. 또 이용자는 상기 액세스장치에 의해 메모리카드에 기록되어 있는 음악 등의 저작물을 취득하고, 취득한 저작물을 퍼스널 컴퓨터(500)에 재생하여 즐긴다고 해도 된다.

(4) 상기 실시예에서는 DES 암호를 인용한다고 하고 있지만 다른 암호를 이용해도 된다.

(5) 메모리카드는 반도체 메모리 대신 광디스크매체나 MO(Magneto-Optical) 매체를 갖는다고 해도 된다.

(6) 상기 실시예에서는 고유키는 제조되는 기록매체장치마다 다른 키정보라고 하고 있지만, 다음과 같이 해도 된다.

복수개의 기록매체장치는 같은 키정보인 고유키를 갖고, 또한 별도의 복수개의 기록매체장치는 별도의 키정보인 고유키를 갖는다고 해도 된다.

또 같은 제조판수를 갖는 기록매체장치는 같은 키정보를 갖고, 다른 제조판수를 갖는 기록매체장치는 다른 키정보를 갖는다고 해도 된다.

또 동일한 제조업자가 제조하는 기록매체장치는 같은 키정보를 갖고, 다른 제조업자가 제조하는 기록매체장치는 다른 키정보를 갖는다고 해도 된다.

(7) 기록매체장치와 액세스장치가 모두 정당성을 갖는다고 인증된 경우에 사용자키를 이용하여 디지털 저작물을 암호화하고, 또는 복호할때 다음에 나타내는 바와 같이 해도 된다.

기록매체장치와 메모리카드 기입기인 액세스장치가 접속되었을 때 상기 액세스장치는 조작자로부터 사용자키의 입력을 접수하고, 디지털 저작물을 구성하는 파일마다 파일키를 생성하여 상기 사용자키와 상기 파일키 사이에 소정의 연산을 실시하여 파일마다 변형키를 생성한다. 여기에서 소정의 연산은 일례로서 배타적 논리합이다. 상기 액세스장치는 생성한 1이상의 변형키를 이용하여 1이상의 상기 파일을 각각 암호화하여 1이상의 암호화파일을 생성하고, 생성한 1이상의 상기 암호화파일과 생성한 1이상의 상기 변형키를 기록매체장치로 출력한다. 상기 기록매체장치는 1이상의 상기 암호화파일과 1이상의 상기 변형키를 수취하여 기억한다.

1이상의 상기 암호화파일과 1이상의 상기 변형키를 기억하고 있는 기록매체장치와 메모리카드 판독기인 액세스장치가 접속되었을 때 상기 기록매체장치는 1이상의 상기 암호화파일과 1이상의 상기 변형키를 상기 액세스장치로 출력하고, 상기 액세스장치는 1이상의 상기 암호화파일과 1이상의 상기 변형키를 수취하고, 조작자로부터 사용자키의 입력을 접수하고, 상기 암호화파일마다 상기 사용자키와 상기 변형키 사이에 상기 소정의 연산의 반대연산을 실시하여 파일키를 생성하고, 생성한 파일키를 이용하여 암호화파일을 복호하여 파일을 생성하고, 생성한 파일을 재생한다.

(8) 다른 실시예는 컴퓨터에 의해 실행하는 프로그램을 기록한 컴퓨터 판독가능한 기록매체로서, 상기 순서를 컴퓨터에 실행시키는 프로그램을 기록하고 있어도 된다. 또 상기 프로그램으로 구성된 컴퓨터 디지털신호라고 해도 된다.

(9) 또 다른 실시예는 상기 프로그램을 통신회선을 통해서 전송하는 전송매체라고 해도 된다. 상기 기록매체를 이송함으로써, 또 상기 프로그램을 통신회선을 통해서 이송함으로써 독립된 다른 컴퓨터 시스템으로 실시하도록 해도 된다. 또 통신회선을 통해 전송되는 상기 컴퓨터 프로그램 또는 상기 컴퓨터 디지털신호라고 해도 된다.

(10) 상기에 설명한 복수의 실시예로부터 몇개의 실시예를 선택하여 조합해도 된다. 또 몇개의 실시예의 일부를 선택하여 조합해도 된다.

발명의 효과

상술한 바와 같은 본 발명의 구성에 의하면 외부로부터 인출된 디지털 저작물을 부정하게 기록매체에 기입하는 것과, 기록매체에 기록된 디지털 제작물을 부정하게 재생하는 것을 방지할 수 있게 된다.

본 발명의 바람직한 실시예들은 예시의 목적을 위해 개시된 것이며, 당업자라면 첨부된 특허청구범위에 개시된 본 발명의 사상과 범위를 통해 각종 수정, 변경, 대체 및 부가가 가능할 것이다.

(57) 청구의 범위

청구항 1

디지털 저작물정보를 기억하는 영역을 갖는 기록매체장치와, 상기 영역으로부터 정보를 판독 또는 상기 영역에 정보를 기입하는 액세스장치로 구성되고, 상기 기록매체장치와 상기 액세스장치 사이에서 디지털 저작물의 이용을 실현하는 디지털 저작물 보호시스템에 있어서,

상기 기록매체장치는 소유하는 고유키를 상기 액세스장치에 비밀 전송하고, 상기 기록매체장치 및 상기 액세스장치는 각각 상기 고유키를 이용하여 상대 장치의 정당성을 인증하는 단계로서, 상기 고유키는 상기 기록매체장치에 고유한 키정보인 인증단계와,

상기 기록매체장치와 상기 액세스장치가 모두 정당성을 갖는다고 인증된 경우에, 상기 액세스장치는 상기 고유키를 이용하여 디지털 저작물을 암호화하여 상기 기록매체장치로 전송하거나 또는 상기 기록매체장치로부터 전송된 암호화된 디지털 저작물을 상기 고유키를 이용하여 복호하는 저작물전송단계를 포함하는 것을 특징으로 하는 디지털 저작물 보호시스템.

청구항 2

제 1항에 있어서,

상기 인증단계에서의 상기 액세스장치에 의한 상기 기록매체장치의 정당성 인증에서,

상기 기록매체장치는 제 1 연산수단을 포함하며,

상기 액세스장치는 제 1 인증정보 생성수단과 제 1 인증수단을 포함하며,

상기 제 1 인증정보 생성수단은 제 1 인증정보를 생성하고, 생성한 상기 제 1 인증정보를 상기 기록매체장치에 출력하며,

상기 제 1 연산수단은 상기 제 1 인증정보를 수취하고, 상기 고유키를 이용하여 상기 제 1 인증정보에 제 1 연산을 실시하여 제 1 연산 인증정보를 생성하고, 생성한 상기 제 1 연산 인증정보를 상기 액세스장치에 출력하며,

상기 제 1 인증수단은 비밀전송된 상기 고유키를 이용하여, 상기 제 1 인증정보와, 상기 제 1 연산 인증정보에 의해 상기 기록매체장치가 정당성을 갖는지의 여부를 인증하는 것을 특징으로 하는 디지털 저작물 보호시스템.

청구항 3

제 2항에 있어서,

상기 인증단계에서의 상기 기록매체장치에 의한 상기 액세스장치의 정당성 인증에서,

상기 액세스장치는 제 2 연산수단을 포함하며,

상기 기록매체장치는 제 2 인증정보 생성수단과 제 2 인증수단을 포함하며,

상기 제 2 인증정보 생성수단은 제 2 인증정보를 생성하고, 생성한 상기 제 2 인증정보를 상기 액세스장치에 출력하며,

상기 제 2 연산수단은 상기 제 2 인증정보를 수취하고, 비밀전송된 상기 고유키를 이용하여 상기 제 2 인증정보에 제 2 연산을 실시하여 제 2 연산 인증정보를 생성하고, 생성한 상기 제 2 연산 인증정보를 상기 기록매체장치에 출력하며,

상기 제 2 인증수단은 상기 고유키를 이용하여, 상기 제 2 인증정보와, 상기 제 2 연산인증정보에 의해 상기 액세스장치가 정당성을 갖는지의 여부를 인증하는 것을 특징으로 하는 디지털 저작물 보호시스템.

청구항 4

제 3항에 있어서,

상기 인증단계에서의 상기 기록매체장치로부터 상기 액세스장치로의 고유키 비밀전송에서,

상기 기록매체장치는,

상기 고유키를 기억하는 고유키 기억수단과,

상기 고유키에 제 1 암호알고리즘을 실시하여 암호화 고유키를 생성하고, 생성한 상기 암호화 고유키를 상기 액세스장치로 출력하는 제 1 암호수단을 포함하며,

상기 액세스장치는,

상기 암호화 고유키를 수취하고, 상기 암호화 고유키에 제 1 복호알고리즘을 실시하여 복호고유키를 생성하는 제 1 복호수단을 포함하고, 상기 제 1 복호알고리즘은 상기 제 1 암호알고리즘에 의해 생성된 암호문을 복호하는 것을 특징으로 하는 디지털 저작물 보호시스템.

청구항 5

제 4항에 있어서,

상기 기록매체장치는 또한 제 1 키를 미리 기억하고 있는 제 1 키 기억수단을 포함하며,

상기 제 1 암호수단은 상기 제 1 키를 이용하여 상기 고유키에 상기 제 1 암호알고리즘을 실시하여 상기 암호화 고유키를 생성하며,

상기 액세스장치는 또한 제 2 키를 미리 기억하고 있는 제 2 키 기억수단을 포함하며, 상기 제 2 키는 상기 제 1 키에 대응하고 있고,

상기 제 1 복호수단은 상기 제 1 키에 대응하는 상기 제 2 키를 이용하여 상기 암호화 고유키에 상기 제 1 복호알고리즘을 실시하여 상기 복호고유키를 생성하는 것을 특징으로 하는 디지털 저작물 보호시스템.

청구항 6

제 5항에 있어서,

상기 제 1 키는 마스터키로서 상기 제 2 키와 동일키이고,

상기 제 2 키는 마스터키이고,

상기 제 1 복호수단은 상기 제 1 키와 동일한 상기 제 2 키를 이용하여 상기 암호화 고유키에 상기 제 1 복호알고리즘을 실시하여 상기 복호고유키를 생성하는 것을 특징으로 하는 디지털 저작물 보호시스템.

청구항 7

제 5항에 있어서,

상기 제 1 키는 상기 제 2 키를 기초로 하여 공개키 암호방식의 공개키 결정알고리즘에 의해 산출되는 공개키이고,

상기 제 1 암호수단은 상기 제 1 키를 이용하여 상기 고유키에 상기 제 1 암호알고리즘을 실시하여 상기

암호화 고유키를 생성하며, 상기 제 1 암호알고리즘은 상기 공개키 암호방식의 암호알고리즘이고,

상기 제 1 복호수단은 상기 제 2 키를 이용하여 상기 암호화 고유키에 상기 제 1 복호알고리즘을 실시하여 상기 복호고유키를 생성하며, 상기 제 1 복호알고리즘은 상기 공개키 암호방식의 복호알고리즘인 것을 특징으로 하는 디지털 저작물 보호시스템.

청구항 8

제 5항에 있어서,

상기 제 2 키는 상기 제 1 키를 기초로 하여 회복형 서명처리방식의 공개키 결정알고리즘에 의해 산출되는 공개키이고,

상기 제 1 암호알고리즘은 상기 회복형 서명처리방식의 서명처리 알고리즘이며,

상기 제 1 암호수단은 상기 제 1 키를 이용하여 상기 고유키에 상기 제 1 암호알고리즘을 실시하여 서명문인 상기 암호화 고유키를 생성하며,

상기 제 1 복호알고리즘은 상기 회복형 서명처리방식의 검증처리 알고리즘이며,

상기 제 1 복호수단은 상기 제 2 키를 이용하여 서명문인 상기 암호화 고유키에 상기 제 1 복호알고리즘을 실시하고, 상기 복호고유키를 생성하는 것을 특징으로 하는 디지털 저작물 보호시스템.

청구항 9

제 4항에 있어서,

상기 기록매체장치는, 또한

복수개의 마스터키로 된 마스터키군을 미리 기억하고 있는 제 1 마스터키 기억수단과,

상기 마스터키군 중에서 하나의 마스터키를 제1 키로서 선택하는 제 1 선택수단을 포함하며,

상기 제 1 암호수단은 선택된 상기 제 1 키를 이용하여 상기 고유키에 상기 제 1 암호알고리즘을 실시하여 상기 암호화 고유키를 생성하며,

상기 액세스장치는, 또한

상기 마스터키군과 동일한 마스터키군을 미리 기억하고 있는 제 2 마스터키 기억수단과,

상기 제 2 마스터키 기억수단에 기억되어 있는 마스터키군 중에서 상기 제 1 키와 동일한 마스터키를 제 2 키로서 선택하는 제 2 선택수단을 포함하며,

상기 제 1 복호수단은 상기 제 1 키와 동일한 상기 제 2 키를 이용하여 상기 암호화 고유키에 상기 제 1 복호알고리즘을 실시하여 상기 복호고유키를 생성하는 것을 특징으로 하는 디지털 저작물 보호시스템.

청구항 10

제 4항에 있어서,

상기 제 1 암호수단은,

서브그룹키를 미리 기억하고 있고,

상기 서브그룹키를 이용하여 상기 고유키에 제 1 변환을 실시하여 변형키를 생성하며,

상기 변형키에 상기 제 1 암호알고리즘을 실시하며, 상기 암호화 고유키를 생성하며,

상기 제 1 복호수단은,

상기 서브그룹키와 동일한 서브그룹키를 미리 기억하고 있고,

상기 암호화 고유키에 상기 제 1 복호알고리즘을 실시하여 복호변형키를 생성하고,

상기 서브그룹키를 이용하여 상기 복호변형키에 상기 제 1 변환의 역변환을 실시하여 복호고유키를 생성하는 것을 특징으로 하는 디지털 저작물 보호시스템.

청구항 11

제 4항에 있어서,

상기 제 1 암호수단은,

서브그룹키를 미리 기억하고 있고,

상기 고유키에 제 1 암호알고리즘을 실시하여 암호문을 생성하고,

상기 서브그룹키를 이용하여 상기 암호문에 제 1 변환을 실시하여 암호화 고유키를 생성하며,

상기 제 1 복호수단은,

상기 서브그룹키와 동일한 서브그룹키를 미리 기억하고 있고,

상기 서브그룹키를 이용하여 상기 암호화 고유키에 상기 제 1 변환의 역변환을 실시하여 복호문을 생성하고,

상기 복호문에 상기 제 1 복호알고리즘을 실시하여 복호고유키를 생성하는 것을 특징으로 하는 디지털 저

작물 보호시스템.

청구항 12

제 4항에 있어서,

상기 기록매체장치는 또한 제 1 키를 미리 기억하고 있는 제 1 키 기억수단을 포함하며, 상기 제 1 키는 마스터키이며,

상기 제 1 암호수단은,

서브그룹키를 미리 기억하고 있고,

상기 서브그룹키를 이용하여 상기 제 1 키에 제 1 변환을 실시하여 암호화 제 1 키를 생성하고,

생성한 상기 암호화 제 1 키를 이용하여 상기 고유키에 상기 제 1 암호알고리즘을 실시하여 상기 암호화 고유키를 생성하며,

상기 액세스장치는 또한 제 2 키를 미리 기억하고 있는 제 2 키 기억수단을 포함하며, 상기 제 2 키는 마스터키로서 상기 제 1 키와 동일키이고,

상기 제 1 복호수단은,

상기 서브그룹키와 동일한 서브그룹키를 미리 기억하고 있고,

상기 서브그룹키를 이용하여 상기 제 2 키에 상기 제 1 변환과 동일한 변환을 실시하여 암호화 제 2 키를 생성하고,

생성한 상기 암호화 제 2 키를 이용하여 상기 암호화 고유키에 상기 제 1 복호알고리즘을 실시하여 상기 복호고유키를 생성하는 것을 특징으로 하는 디지털 저작물 보호시스템.

청구항 13

제 3항에 있어서,

상기 제 1 인증수단은,

비밀전송된 상기 고유키를 이용하여 상기 제 1 인증정보에 상기 제 1 연산과 동일한 연산을 실시하여 제 3 연산인증정보를 생성하는 제 3 연산수단과,

상기 제 1 연산인증정보와 상기 제 3 연산인증정보가 일치하는지의 여부를 판단하여 일치하는 경우에 상기 기록매체장치가 정당성을 갖는다고 인증하는 제 1 비교수단을 포함하는 것을 특징으로 하는 디지털 저작물 보호시스템.

청구항 14

제 13항에 있어서,

상기 제 2 인증수단은,

상기 고유키를 이용하여 상기 제 2 인증정보에 상기 제 2 연산과 동일한 연산을 실시하여 제 4 연산인증정보를 생성하는 제 4 연산수단과,

상기 제 2 연산인증정보와 상기 제 4 연산인증정보가 일치하는지의 여부를 판단하여 일치하는 경우에 상기 액세스장치가 정당성을 갖는다고 인증하는 제 2 비교수단을 포함하는 것을 특징으로 하는 디지털 저작물 보호시스템.

청구항 15

제 14항에 있어서,

상기 제 1 연산수단은,

서브그룹키를 미리 기억하고 있고,

상기 서브그룹키를 이용하여 상기 고유키에 제 1 변환을 실시하여 변형고유키를 생성하며,

생성한 상기 변형고유키를 이용하여 상기 제 1 인증정보에 상기 제 1 연산을 실시하여 상기 제 1 연산인증정보를 생성하며,

상기 제 3 연산수단은,

상기 서브그룹키와 동일한 서브그룹키를 미리 기억하고 있고,

상기 서브그룹키를 이용하여 비밀전송된 상기 고유키에 상기 제 1 변환의 역변환을 실시하여 변형복호 고유키를 생성하고,

생성한 상기 변형복호 고유키를 이용하여 상기 제 1 인증정보에 상기 제 1 연산과 동일한 연산을 실시하여 상기 제 3 연산인증정보를 생성하는 것을 특징으로 하는 디지털 저작물 보호시스템.

청구항 16

제 14항에 있어서,

상기 제 1 인증정보 생성수단은 난수를 생성하며, 생성한 난수를 제 1 인증정보로 하고,

상기 제 2 인증정보 생성수단은 난수를 생성하며, 생성한 난수를 제 2 인증정보로 하는 것을 특징으로 하는 디지털 저작물 보호시스템.

청구항 17

제 3항에 있어서,

상기 제 1 연산은 제 1 암호알고리즘이고,

상기 제 1 연산수단은 상기 고유키를 이용하여 상기 제 1 인증정보에 상기 제 1 암호알고리즘을 실시하여 제 1 연산인증정보를 생성하며,

상기 제 1 인증수단은 비밀전송된 상기 고유키를 이용하여 상기 제 1 연산인증정보에 제 1 복호알고리즘을 실시하여 제 1 복호화 인증정보를 생성하고, 상기 제 1 인증정보와 상기 제 1 복호화 인증정보와가 일치하는지의 여부를 판단하며 일치하는 경우에 상기 기록매체장치가 정당성을 갖는다고 인증하며, 여기에서 상기 제 1 복호알고리즘은 상기 제 1 암호알고리즘에 의해 생성된 암호문을 복호하는 것을 특징으로 하는 디지털 저작물 보호시스템.

청구항 18

제 17항에 있어서,

상기 제 2 연산은 제 2 암호알고리즘이고,

상기 제 2 연산수단은 비밀전송된 상기 고유키를 이용하여 상기 제 2 인증정보에 상기 제 2 암호알고리즘을 실시하여 제 2 연산인증정보를 생성하고,

상기 제 2 인증수단은 상기 고유키를 이용하여 상기 제 2 연산인증정보에 제 2 복호알고리즘을 실시하여 제 2 복호화 인증정보를 생성하고, 상기 제 2 인증정보와 상기 제 2 복호화 인증정보가 일치하는지의 여부를 판단하여 일치하는 경우에 상기 액세스장치가 정당성을 갖는다고 인증하며, 상기 제 2 복호알고리즘은 상기 제 2 암호알고리즘에 의해 생성된 암호문을 복호하는 것을 특징으로 하는 디지털 저작물 보호시스템.

청구항 19

제 18항에 있어서,

상기 제 1 연산수단은,

서브그룹키를 미리 기억하고 있고,

상기 서브그룹키를 이용하여 상기 고유키에 제 1 변환을 실시하여 변형고유키를 생성하여 생성한 상기 변형고유키를 이용하여 상기 제 1 인증정보에 상기 제 1 암호알고리즘을 실시하여 상기 제 1 연산인증정보를 생성하며,

상기 제 1 인증수단은,

상기 서브그룹키와 동일한 서브그룹키를 미리 기억하고 있고,

상기 서브그룹키를 이용하여 비밀전송된 상기 고유키에 상기 제 1 변환의 역변환을 실시하여 변형복호 고유키를 생성하며,

생성한 상기 변형복호 고유키를 이용하여 상기 제 1 인증정보에 상기 제 1 복호알고리즘을 실시하여 상기 제 1 복호화 인증정보를 생성하는 것을 특징으로 하는 디지털 저작물 보호시스템.

청구항 20

제 18항에 있어서,

상기 제 1 인증정보 생성수단은 난수를 생성하고, 생성한 난수를 제 1 인증정보로 하며,

상기 제 2 인증정보 생성수단은 난수를 생성하고, 생성한 난수를 제 2 인증정보로 하는 것을 특징으로 하는 디지털 저작물 보호시스템.

청구항 21

제 3항에 있어서,

상기 저작물 전송단계에서,

상기 기록매체장치는,

디지털 저작물정보를 기억하고 있고, 상기 디지털 저작물정보는 상기 고유키를 이용하여 디지털 저작물에 암호알고리즘이 실시되어 생성되어 있는 상기 영역과,

상기 기록매체장치와 상기 액세스장치가 모두 정당성을 가지면 인증된 경우에 상기 영역으로부터 상기 디지털 저작물정보를 판독하고, 판독한 상기 디지털 저작물정보를 상기 액세스장치로 출력하는 출력수단을 포함하며,

상기 영역으로부터 정보를 판독하는 상기 액세스장치는,

상기 기록매체장치로부터 상기 디지털 저작물정보를 수취하고, 상기 비밀전송된 고유키를 이용하여 수취한 상기 디지털 저작물정보에 복호알고리즘을 실시하여 복호디지털 저작물을 생성하는 저작물 복호수단으

로서, 상기 복호알고리즘은 상기 암호알고리즘에 의해 생성된 암호문을 복호하는 저작물 복호수단과,

생성된 상기 복호디지털 저작물을 재생하는 재생수단을 포함하는 것을 특징으로 하는 디지털 저작물 보호 시스템.

청구항 22

제 3항에 있어서,

상기 저작물 전송단계에서,

상기 영역으로 정보를 기입하는 상기 액세스장치는,

외부로부터 디지털 저작물을 취득하는 저작물 취득수단과,

상기 비밀전송된 고유키를 이용하여 상기 취득한 디지털 저작물에 암호알고리즘을 실시하여 디지털 저작물정보를 생성하고, 상기 기록매체장치로 출력하는 저작물 암호화수단을 포함하며,

상기 기록매체장치는,

상기 디지털 저작물정보를 수취하고, 수취한 상기 디지털 저작물정보를 기억하는 상기 영역을 포함하는 것을 특징으로 하는 디지털 저작물 보호시스템.

청구항 23

제 1항에 있어서,

상기 저작물 전송단계에서,

상기 기록매체장치와 상기 액세스장치가 모두 정당성을 갖는다고 인증된 경우에, 상기 액세스장치는,

상기 디지털 저작물을 분할하여 1이상의 데이터블록을 생성하고, 생성한 상기 데이터블록마다 데이터블록키를 생성하고, 상기 고유키와 상기 데이터블록에 대응하는 상기 데이터블록키를 이용하여 상기 데이터블록을 암호화하여 암호화 데이터블록을 생성하며, 생성한 암호화 데이터블록을 상기 기록매체장치로 전송하며,

혹은 상기 기록매체장치로부터 상기 암호화된 디지털 저작물을 구성하는 1이상의 암호화 데이터블록을 수신하고, 수신한 상기 암호화 데이터블록마다 데이터블록키를 생성하고, 상기 고유키와 상기 암호화 데이터블록에 대응하는 상기 데이터블록키를 이용하여 수신한 상기 암호화 데이터블록을 복호하여 데이터블록을 생성하며,

여기에서 상기 데이터블록은 논리적 단위길이 혹은 물리적 단위길이를 갖고, 상기 암호화 데이터블록은 논리적 단위길이 혹은 물리적 단위길이를 갖는 것을 특징으로 하는 디지털 저작물 보호시스템.

청구항 24

제 1항에 있어서,

상기 저작물 전송단계에서,

상기 기록매체장치와 상기 액세스장치가 모두 정당성을 갖는다고 인증된 경우에, 상기 액세스장치는,

상기 디지털 저작물을 구성하는 파일마다 파일키를 생성하고, 상기 고유키와 상기 파일키를 이용하여 상기 파일을 암호화하여 암호화파일을 생성하며, 생성한 암호화파일과 파일키에 관한 정보를 상기 기록매체장치로 전송하며,

혹은 상기 기록매체장치로부터 상기 암호화된 디지털 저작물을 구성하는 파일과 파일키에 관한 정보를 수신하고, 수신한 파일마다 상기 고유키와 상기 파일키에 관한 정보를 이용하여 수신한 상기 파일을 복호함으로써 디지털 저작물을 재생하는 것을 특징으로 하는 디지털 저작물 보호시스템.

청구항 25

제 24항에 있어서,

상기 저작물 전송단계에서,

상기 기록매체장치와 상기 액세스장치가 모두 정당성을 갖는다고 인증된 경우에, 상기 액세스장치는,

상기 디지털 저작물을 구성하는 파일마다 파일키를 생성하고, 상기 파일키를 이용하여 상기 파일을 암호화하여 암호화파일을 생성하며, 상기 고유키를 이용하여 상기 파일키를 암호화하여 암호화 파일키를 생성하고, 생성한 암호화파일과 암호화 파일키를 상기 기록매체장치로 전송하며,

혹은 상기 기록매체장치로부터 상기 디지털 저작물을 구성하는 파일이 암호화된 암호화파일과, 파일마다 생성된 파일키가 암호화된 암호화 파일키를 수신하고, 수신한 암호화파일마다 상기 고유키를 이용하여 암호화 파일키를 복호하여 파일키를 생성하고, 생성한 파일키를 이용하여 수신한 상기 암호화파일을 복호하여 파일을 생성함으로써 디지털 저작물을 재생하는 것을 특징으로 하는 디지털 저작물 보호시스템.

청구항 26

제 24항에 있어서,

상기 기록매체장치는 현시각을 기초로 하여 시드(seed)를 생성하고, 상기 액세스장치로 출력하며, 여기에서 시드는 난수의 초기값이며,

상기 액세스장치는 상기 시드를 수취하고, 상기 시드를 초기값으로 하여 난수를 생성하고, 생성한 난수를 파일키로 하는 것을 특징으로 하는 디지털 저작물 보호시스템.

청구항 27

제 24항에 있어서,

A. 상기 인증단계에서의 상기 액세스장치에 의한 상기 기록매체장치의 정당성 인증에서,

a. 상기 액세스장치는 제 1 인증정보를 상기 기록매체장치에 전송하고,

b. 상기 기록매체장치는 현시각을 기초로 하여 시드를 생성하고, 상기 시드와 제 1 인증정보를 결합하고, 상기 고유키를 이용하여 상기 시드와 제 1 인증정보의 결합결과에 암호를 실시하여 상기 액세스장치에 전송하며, 여기에서 시드는 난수의 초기값이며,

c. 상기 액세스장치는 비밀전송된 상기 고유키를 이용하여 암호를 실시된 상기 시드와 제 1 인증정보의 결합결과를 복호하여 복호 시드와 제 1 복호인증정보를 생성하고, 상기 제 1 인증정보와 상기 제 1 복호인증정보가 일치하는 경우에 상기 기록매체장치가 정당성을 갖는다고 인증하며,

B. 상기 저작물 전송단계에서,

상기 액세스장치는 상기 복호 시드를 초기값으로 하여 난수를 생성하고, 생성한 난수를 파일키로 하는 것을 특징으로 하는 디지털 저작물 보호시스템.

청구항 28

제 1항에 있어서,

상기 저작물 전송단계에서,

상기 기록매체장치와 상기 액세스장치가 모두 정당성을 갖는다고 인증된 경우에, 상기 액세스장치는,

조작자로부터 사용자키의 입력을 접수하고, 상기 입력을 접수한 사용자키와, 기억매체로부터 비밀전송된 고유키를 기초로 하여 변형키를 생성하고,

상기 변형키를 이용하여 상기 디지털 저작물을 암호화하여 상기 기록매체장치로 전송하며,

혹은 상기 기록매체장치로부터 상기 암호화된 디지털 저작물을 수신하고, 상기 변형키를 이용하여, 수신한 암호화된 디지털 저작물을 복호하여 디지털 저작물을 생성하는 것을 특징으로 하는 디지털 저작물 보호시스템.

청구항 29

제 1항에 있어서,

상기 저작물 전송단계에서,

상기 기록매체장치와 상기 액세스장치가 모두 정당성을 갖는다고 인증된 경우에, 상기 액세스장치는,

조작자로부터 사용자키의 입력을 접수하고, 상기 디지털 저작물을 구성하는 파일마다 파일키를 생성하며, 상기 사용자키와 상기 파일키를 기초로 하여 변형키를 생성하고, 상기 변형키를 이용하여 상기 파일을 암호화하고 암호화파일을 생성하며, 생성한 암호화파일과 상기 변형키를 상기 기록매체장치로 전송하며,

혹은 상기 디지털 저작물을 구성하는 파일이 암호화된 암호화파일과, 상기 사용자키와 상기 파일키를 기초로 하여 생성된 변형키를 수신하며 조작자로부터 사용자키의 입력을 접수하고, 상기 사용자키와 상기 변형키를 기초로 하여 파일키를 생성하고, 상기 파일키를 이용하여 수신한 상기 암호화파일을 복호하여 파일을 생성함으로써 디지털 저작물을 재생하는 것을 특징으로 하는 디지털 저작물 보호시스템.

청구항 30

제 1항에 있어서,

A. 상기 인증단계에서의 상기 기록매체장치에 의한 상기 액세스장치의 정당성 인증에서,

a. 상기 기록매체장치는 제 2 인증정보를 상기 액세스장치에 전송하고,

b. 상기 액세스장치는 마스터키를 이용하여 상기 제 2 인증정보에 암호를 실시하여 상기 기록매체장치에 전송하고,

c. 상기 기록매체장치는 마스터키를 이용하여 암호를 실시한 상기 제 2 인증정보를 복호하여, 제 2 복호인증정보를 생성하고, 상기 제 2 인증정보와 상기 제 2 복호인증정보가 일치하는 경우에 상기 액세스장치가 정당성을 갖는다고 인증하는 것을 특징으로 하는 디지털 저작물 보호시스템.

청구항 31

제 1항에 있어서,

암호화 고유키 작성장치가 추가로 포함되고,

디지털 저작물 보호시스템은,

상기 암호화 고유키 작성장치는 상기 기록매체장치가 소유하는 고유키에 암호를 실시하여 암호화 고유키를 생성하고, 상기 기록매체장치는 상기 생성된 암호화 고유키를 기억하는 암호화 고유키 설정단계를 가

지며,

상기 인증단계에서,

상기 기록매체장치는 기억하고 있는 암호화 고유키를 상기 액세스장치에 전송하고, 상기 액세스장치는 취득한 상기 암호화 고유키를 복호하여 고유키를 생성하며, 생성한 상기 고유키를 이용하여 상기 기록매체장치의 정당성을 인증하는 것을 특징으로 하는 디지털 저작물 보호시스템.

청구항 32

디지털 저작물정보를 기억하는 영역을 갖는 기록매체장치에 있어서,

상기 기록매체장치는 디지털 저작물 보호시스템을 구성하는 구성요소이며,

상기 디지털 저작물 보호시스템은 상기 기록매체장치와, 상기 영역으로부터 정보를 판독하거나 또는 상기 영역으로 정보를 기입하는 액세스장치로 구성되며, 상기 기록매체장치와 상기 액세스장치 사이에 있어 디지털 저작물의 이용을 실현하고,

상기 기록매체장치는 소유하는 고유키를 상기 액세스장치에 비밀 전송하고, 상기 기록매체장치 및 상기 액세스장치는 각각 상기 고유키를 이용하여 상대 장치의 정당성을 인증하며, 상기 고유키는 상기 기록매체장치에 고유의 키정보인 인증단계와,

상기 기록매체장치와 상기 액세스장치가 모두 정당성을 갖는다고 인증된 경우에, 상기 액세스장치는 상기 고유키를 이용하여 디지털 저작물을 암호화하여 상기 기록매체장치로 전송하고, 혹은 상기 기록매체장치로부터 전송된 암호화된 디지털 저작물을 상기 고유키를 이용하여 복호하는 저작물 전송단계를 갖는 것을 특징으로 하는 기록매체장치.

청구항 33

제 32항에 있어서,

상기 인증단계에서의 상기 액세스장치에 의한 상기 기록매체장치의 정당성 인증에서,

상기 기록매체장치는 제 1 연산수단을 포함하며,

상기 액세스장치는 제 1 인증정보 생성수단과 제 1 인증수단을 포함하며,

상기 제 1 인증정보 생성수단은 제 1 인증정보를 생성하고, 생성한 상기 제 1 인증정보를 상기 기록매체장치에 출력하며,

상기 제 1 연산수단은 상기 제 1 인증정보를 수취하고, 상기 고유키를 이용하여 상기 제 1 인증정보에 제 1 연산을 실시하여 제 1 연산인증정보를 생성하고, 생성한 상기 제 1 연산인증정보를 상기 액세스장치에 출력하며,

상기 제 1 인증수단은 비밀전송된 상기 고유키를 이용하여 상기 제 1 인증정보와, 상기 제 1 연산인증정보에 의해 상기 기록매체장치가 정당성을 갖는지의 여부를 인증하는 것을 특징으로 하는 기록매체장치.

청구항 34

제 33항에 있어서,

상기 인증단계에서의 상기 기록매체장치에 의한 상기 액세스장치의 정당성 인증에서,

상기 액세스장치는 제 2 연산수단을 포함하며,

상기 기록매체장치는 제 2 인증정보 생성수단과 제 2 인증수단을 포함하며,

상기 제 2 인증정보 생성수단은 제 2 인증정보를 생성하고, 생성한 상기 제 2 인증정보를 상기 액세스장치에 출력하며,

상기 제 2 연산수단은 상기 제 2 인증정보를 수취하고, 비밀전송된 상기 고유키를 이용하여 상기 제 2 인증정보에 제 2 연산을 실시하여 제 2 연산인증정보를 생성하고, 생성한 상기 제 2 연산인증정보를 상기 기록매체장치에 출력하며,

상기 제 2 인증수단은 상기 고유키를 이용하여 상기 제 2 인증정보와 상기 제 2 연산인증정보에 의해 상기 액세스장치가 정당성을 갖는지의 여부를 인증하는 것을 특징으로 하는 기록매체장치.

청구항 35

디지털 저작물정보를 기억하는 영역을 갖는 기록매체장치의 상기 영역에서 정보를 판독 또는 상기 영역으로 정보를 기입하는 액세스장치에 있어서,

상기 액세스장치는 디지털 저작물 보호시스템을 구성하는 구성요소이고,

상기 디지털 저작물 보호시스템은 상기 기록매체장치와, 상기 액세스장치로 구성되어 상기 기록매체장치와 상기 액세스장치 사이에서 디지털 저작물의 이용을 실현하고,

상기 기록매체장치는 소유하는 고유키를 상기 액세스장치에 비밀 전송하고, 상기 기록매체장치 및 상기 액세스장치는 각각 상기 고유키를 이용하여 상대 장치의 정당성을 인증하며, 상기 고유키는 상기 기록매체장치에 고유의 키정보인 인증단계와,

상기 기록매체장치와 상기 액세스장치가 모두 정당성을 갖는다고 인증된 경우에, 상기 액세스장치는 상기 고유키를 이용하여 디지털 저작물을 암호화하여 상기 기록매체장치로 전송하고, 혹은 상기 기록매체장치

로부터 전송된 암호화된 디지털 저작물을 상기 고유키를 이용하여 복호하는 저작물전송단계를 갖는 것을 특징으로 하는 액세스장치.

청구항 36

제 35항에 있어서,

상기 인증단계에서의 상기 액세스장치에 의한 상기 기록매체장치의 정당성 인증에서,

상기 기록매체장치는 제 1 연산수단을 포함하며,

상기 액세스장치는 제 1 인증정보 생성수단과 제 1 인증수단을 포함하며;

상기 제 1 인증정보 생성수단은 제 1 인증정보를 생성하고, 생성한 상기 제 1 인증정보를 상기 기록매체장치에 출력하며,

상기 제 1 연산수단은 상기 제 1 인증정보를 수취하고, 상기 고유키를 이용하여 상기 제 1 인증정보에 제 1 연산을 실시하여 제 1 연산인증정보를 생성하고, 생성한 상기 제 1 연산인증정보를 상기 액세스장치에 출력하며,

상기 제 1 인증수단은 비밀전송된 상기 고유키를 이용하여 상기 제 1 인증정보와, 상기 제 1 연산인증정보에 의해 상기 기록매체장치가 정당성을 갖는지의 여부를 인증하는 것을 특징으로 하는 액세스장치.

청구항 37

제 36항에 있어서,

상기 인증단계에서의 상기 기록매체장치에 의한 액세스장치의 정당성 인증에서,

상기 액세스장치는 제 2 연산수단을 포함하며,

상기 기록매체장치는 제 2 인증정보 생성수단과 제 2 인증수단을 포함하며,

상기 제 2 인증정보 생성수단은 제 2 인증정보를 생성하고, 생성한 상기 제 2 인증정보를 상기 액세스장치에 출력하며,

상기 제 2 연산수단은 상기 제 2 인증정보를 수취하고, 비밀전송된 상기 고유키를 이용하여 상기 제 2 인증정보에 제 2 연산을 실시하여 제 2 연산인증정보를 생성하고, 생성한 상기 제 2 연산인증정보를, 상기 기록매체장치에 출력하며,

상기 제 2 인증수단은 상기 고유키를 이용하여 상기 제 2 인증정보와 상기 제 2 연산인증정보에 의해 상기 액세스장치가 정당성을 갖는지의 여부를 인증하는 것을 특징으로 하는 액세스장치.

청구항 38

암호화 고유키 작성장치에 있어서,

상기 암호화 고유키 작성장치는 디지털 저작물 보호시스템을 구성하는 구성요소이며,

상기 디지털 저작물 보호시스템은 상기 암호화 고유키 작성장치와, 암호화된 디지털 저작물을 기억하는 영역을 갖는 기록매체장치와, 상기 영역으로부터 정보를 판독 또는 상기 영역으로 정보를 기입하는 액세스장치로 구성되고, 상기 기록매체장치와 상기 액세스장치 사이에서 디지털 저작물의 이용을 실현하고,

상기 암호화 고유키 작성장치는 상기 기록매체장치가 소유하는 고유키에 암호를 실시하여 암호화 고유키를 생성하고, 상기 기록매체장치는 상기 생성된 암호화 고유키를 기억하며, 상기 고유키는 상기 기록매체장치에 고유의 키정보인 암호화 고유키 설정단계와,

상기 기록매체장치는 기억하고 있는 암호화 고유키를 상기 액세스장치에 전송하고, 상기 액세스장치는 취득한 상기 암호화 고유키를 복호하여 고유키를 생성하며, 생성한 상기 고유키를 이용하여 상기 기록매체장치의 정당성을 인증하고, 상기 기록매체장치는 상기 고유키를 이용하여 상기 액세스장치의 정당성을 인증하는 인증단계와,

상기 기록매체장치와 상기 액세스장치가 모두 정당성을 갖는다고 인증된 경우에, 상기 액세스장치는 상기 고유키를 이용하여 디지털 저작물을 암호화하여 상기 기록매체장치로 전송하고, 혹은 상기 기록매체장치로부터 전송된 암호화된 디지털 저작물을 상기 고유키를 이용하여 복호하는 저작물 전송단계를 포함하는 것을 특징으로 하는 암호화 고유키 작성장치.

청구항 39

디지털 저작물정보를 기억하는 영역을 갖는 기록매체장치와, 상기 영역에서 정보를 판독 또는 상기 영역으로 정보를 기입하는 액세스장치로 구성되며, 상기 기록매체장치와 상기 액세스장치 사이에서 디지털 저작물의 이용을 실현하는 디지털 저작물 보호시스템에서 이용되는 디지털 저작물 보호방법에 있어서,

상기 기록매체장치가 소유하는 고유키가 상기 액세스장치에 비밀전송되고, 상기 기록매체장치 및 상기 액세스장치에 의해 상기 고유키를 이용하여 상대장치의 정당성의 인증이 행해지며, 상기 고유키는 상기 기록매체장치에 고유의 키정보인 인증단계와,

상기 기록매체장치와 상기 액세스장치가 모두 정당성을 갖는다고 인증된 경우에 상기 액세스장치에 있어서, 상기 고유키를 이용하여 디지털 저작물이 암호화되며 상기 기록매체장치로 전송되고, 혹은 상기 기록매체장치로부터 전송된 암호화된 디지털 저작물이 상기 고유키를 이용하여 복호되는 저작물 전송단계를 포함하는 것을 특징으로 하는 디지털 저작물 보호방법.

청구항 40

컴퓨터 판독가능한 기록매체상에 기록되어 있는 컴퓨터 프로그램에 있어서,

디지털 저작물정보를 기억하는 영역을 갖는 기록매체장치와, 상기 영역으로부터 정보를 판독 또는 상기 영역으로 정보를 기입하는 액세스장치로 구성되고, 상기 기록매체장치와 상기 액세스장치 사이에서 디지털 저작물의 이용을 실현하는 디지털 저작물 보호시스템에 이용되는 디지털 저작물 보호 프로그램은,

상기 기록매체장치가 소유하는 고유키가 상기 액세스장치에 비밀전송되고, 상기 기록매체장치 및 상기 액세스장치에 의해 각각 상기 고유키를 이용하여 상대 장치의 정당성의 인증이 행해지며, 상기 고유키는 상기 기록매체장치에 고유의 키정보인 인증관계와,

상기 기록매체장치와 상기 액세스장치가 모두 정당성을 갖는다고 인증된 경우에 상기 액세스장치에 있어서, 상기 고유키를 이용하여 디지털 저작물이 암호화되어 상기 기록매체장치로 전송되고, 혹은 상기 기록매체장치로부터 전송된 암호화된 디지털 저작물이 상기 고유키를 이용하여 복호되는 저작물 전송단계를 포함하는 것을 특징으로 하는 디지털 저작물 보호프로그램.

청구항 41

통신회선을 통해 전송되는 컴퓨터 프로그램으로 이루어지는 컴퓨터 디지털신호에 있어서, 상기 컴퓨터 프로그램은 디지털 저작물정보를 기억하는 영역을 갖는 기록매체장치와, 상기 영역으로부터 정보를 판독 또는 상기 영역으로 정보를 기입하는 액세스장치로 구성되며, 상기 기록매체장치와 상기 액세스장치 사이에서 디지털 저작물의 이용을 실현하는 디지털 저작물 보호시스템에서 이용되는 디지털 저작물 보호 프로그램이며,

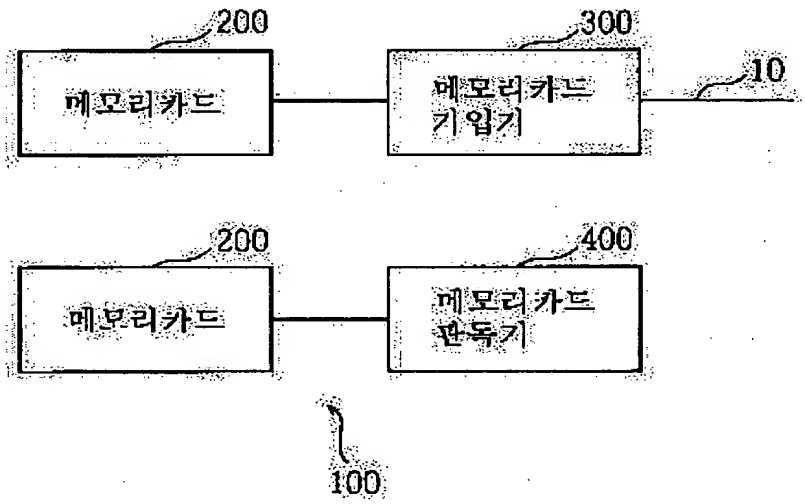
상기 프로그램은,

상기 기록매체장치가 소유하는 고유키가 상기 액세스장치에 비밀전송되고, 상기 기록매체장치 및 상기 액세스장치에 의해 각각 상기 고유키를 이용하여 상대장치의 정당성의 인증이 행해지며, 상기 고유키는 상기 기록매체장치에 고유의 키정보인 인증단계와,

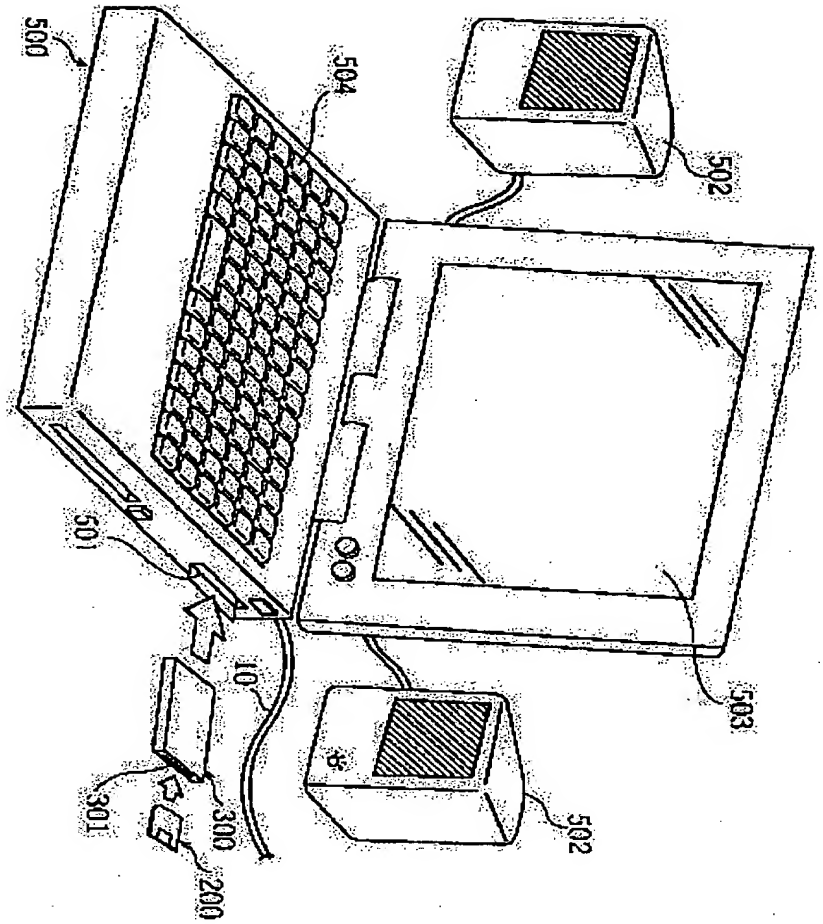
상기 기록매체장치와 상기 액세스장치가 모두 정당성을 갖는다고 인증된 경우에, 상기 액세스장치에서 상기 고유키를 이용하여 디지털 저작물이 암호화되어 상기 기록매체장치로 전송되고, 혹은 상기 기록매체장치로부터 전송된 암호화된 디지털 저작물이 상기 고유키를 이용하여 복호되는 저작물 전송단계를 포함하는 것을 특징으로 하는 디지털 저작물 보호프로그램.

도면

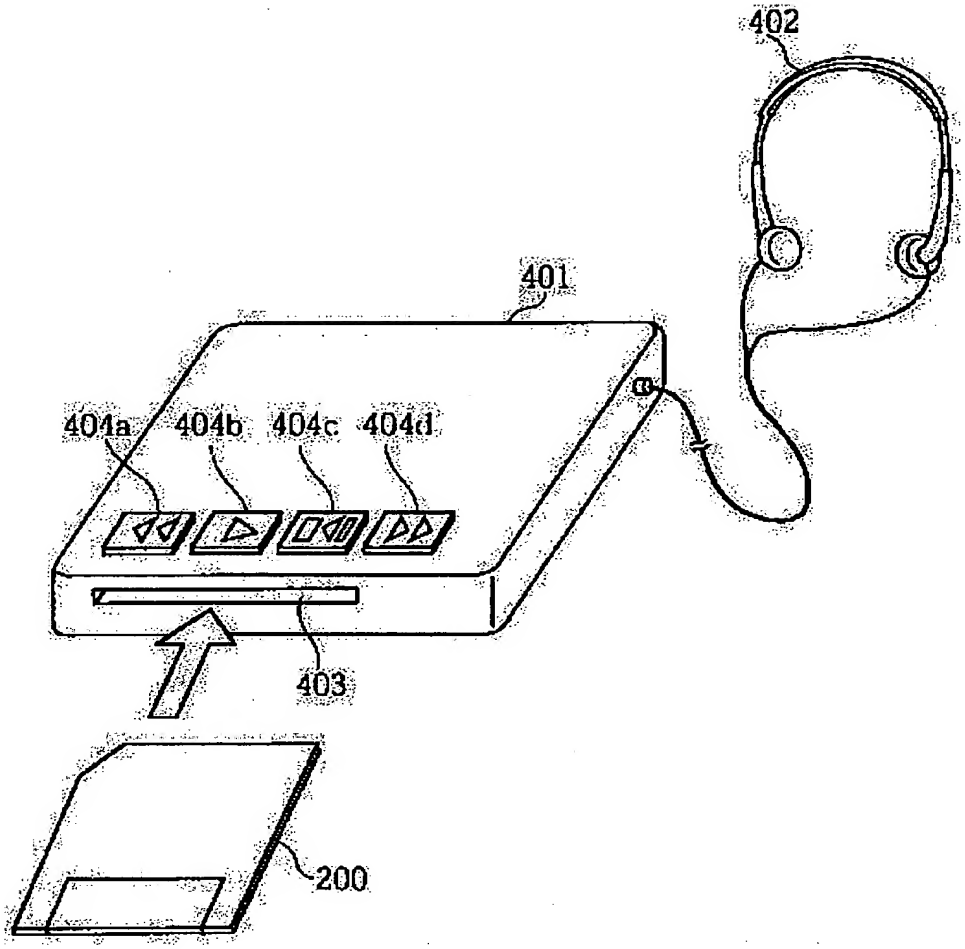
도면1



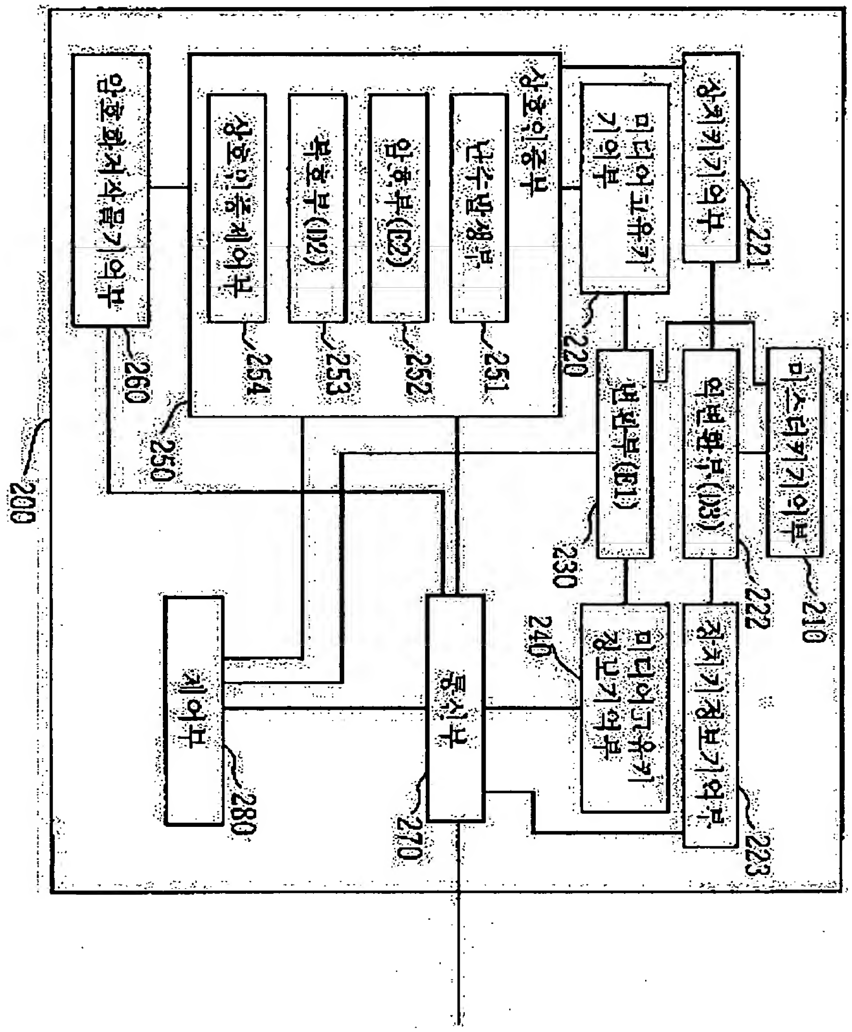
도면2



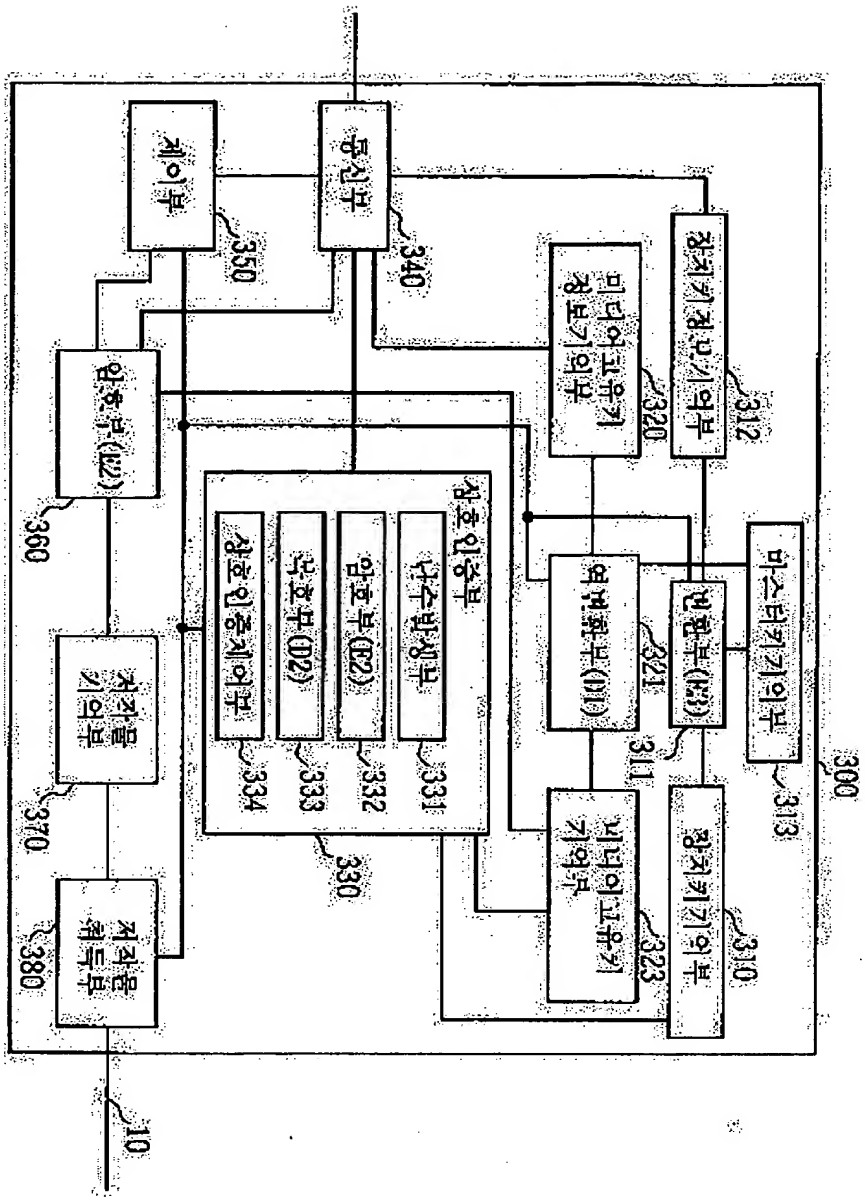
도면3



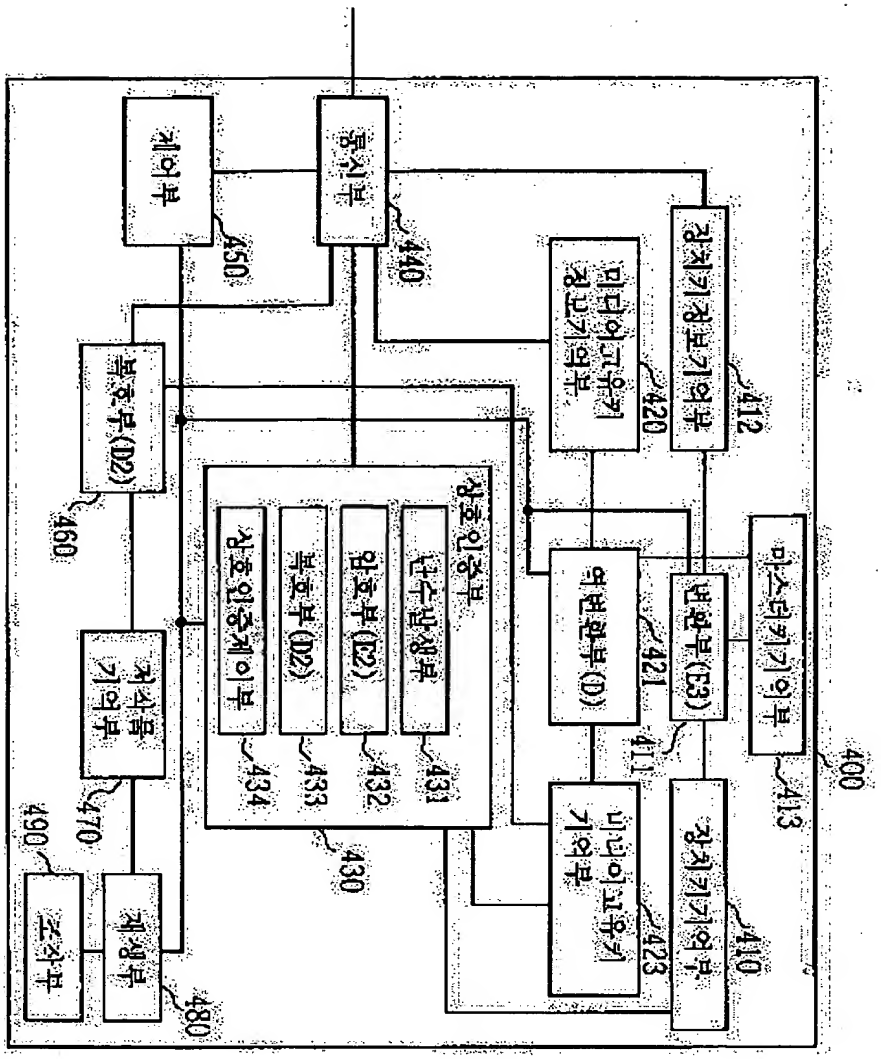
도면4


200
마스터키기억부
210
장치키기억부
221
역변환부(D3)
222
장치키정보기억부
223
미디어고유키기억부
220
변환부(E1)
230
미디어고유키정보기억부
240
상호인증부
250
난수발생부
251
암호부(E2)
252
복호부(D2)
253
상호인증제어부
254
암호화계산물기억부
260
통신부
270
제어부
280

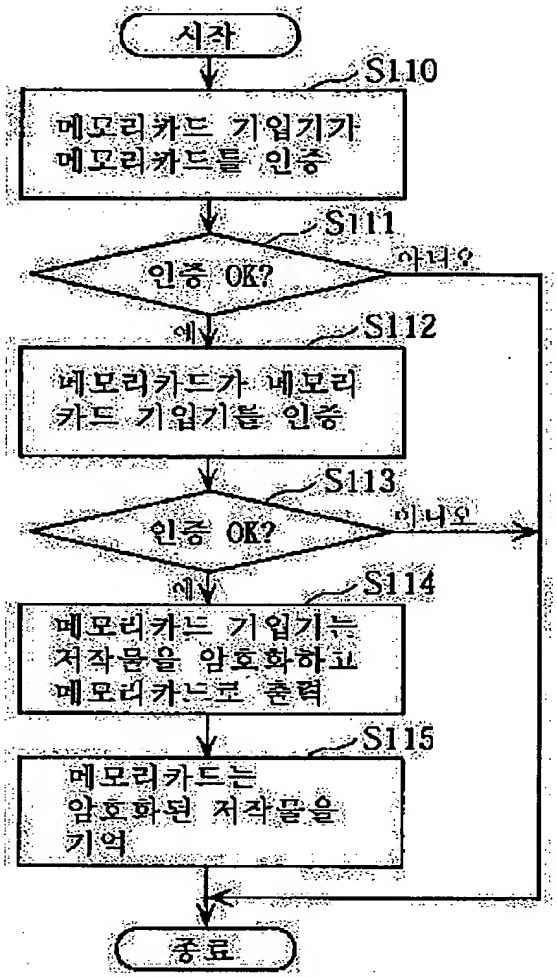
도면5


300
310
311
312
313
320
321
323
330
331
332
333
334
340
350
360
370
380
10
제어부
통신부
암호부(K2)
저장매체 인식부
저장매체 제어부
암호화부(K1)
복호부(K1)
암호인증부
난수발생부
암호부(K2)
복호부(K2)
암호인증제어부
미디어고유키 생성부
저장매체 고유키 생성부
미디어고유키 저장부
저장매체 고유키 저장부

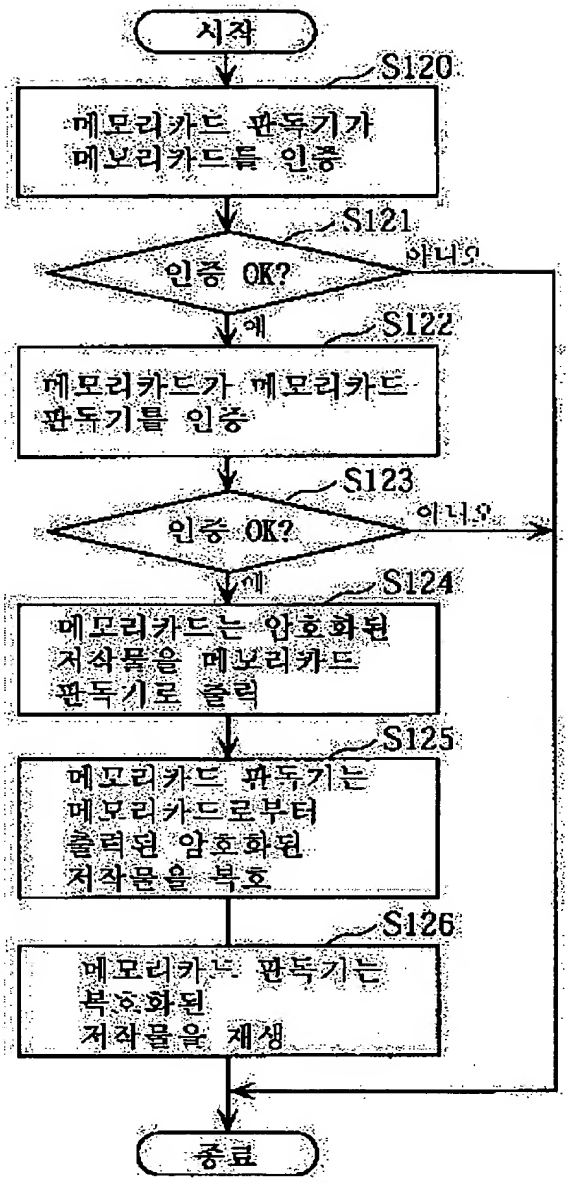
도면6


400
410
강치키기억부
411
변환부(C3)
412
강치키정보기억부
413
마스터키기억부
420
미디어고유키정보기억부
421
역변환부(D)
423
미디어고유키기억부
430
상호인증부
431
난수발생부
432
암호부(E2)
433
복호부(D2)
434
상호인증제어부
440
통신부
450
제어부
460
복호부(D2)
470
저속읽기억부
480
제생부
490
조작부

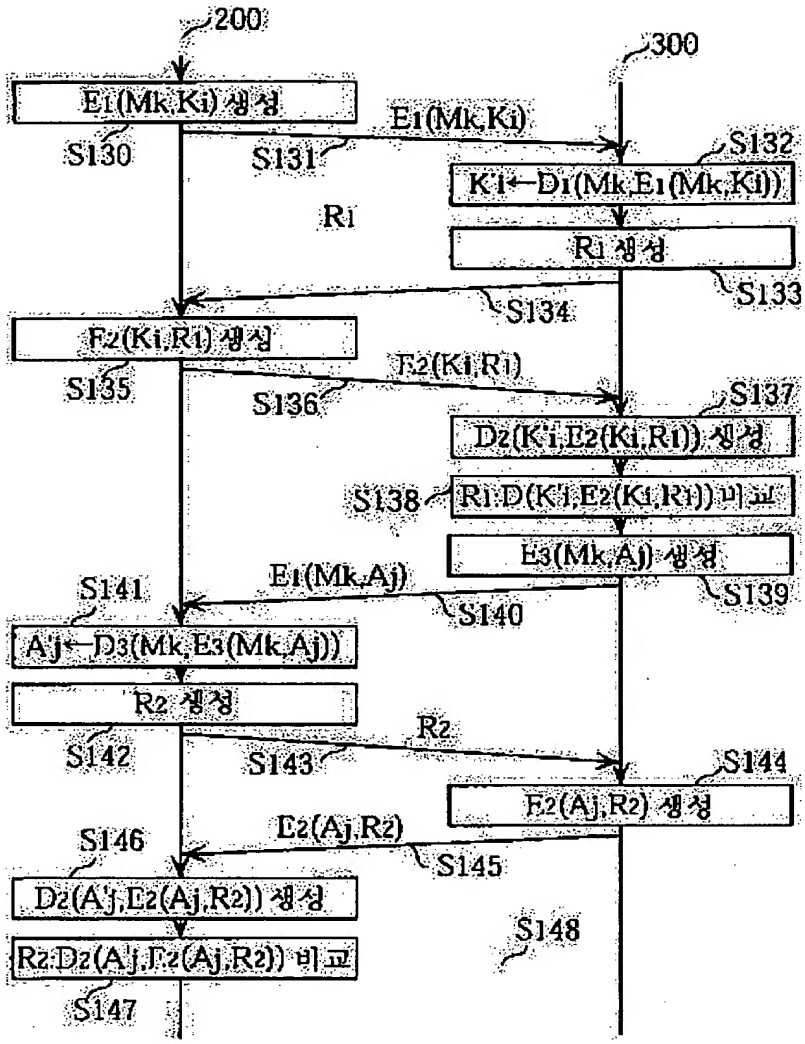
도면7


시작
S110
메모리카드 기입기가 메모리카드를 인증
S111
인증 OK?
아니오
예
S112
메모리카드가 메모리 카드 기입기를 인증
S113
인증 OK?
아니오
예
S114
메모리카드 기입기는 저작물을 암호화하고 메모리카드로 출력
S115
메모리카드는 암호화된 저작물을 기억
종료

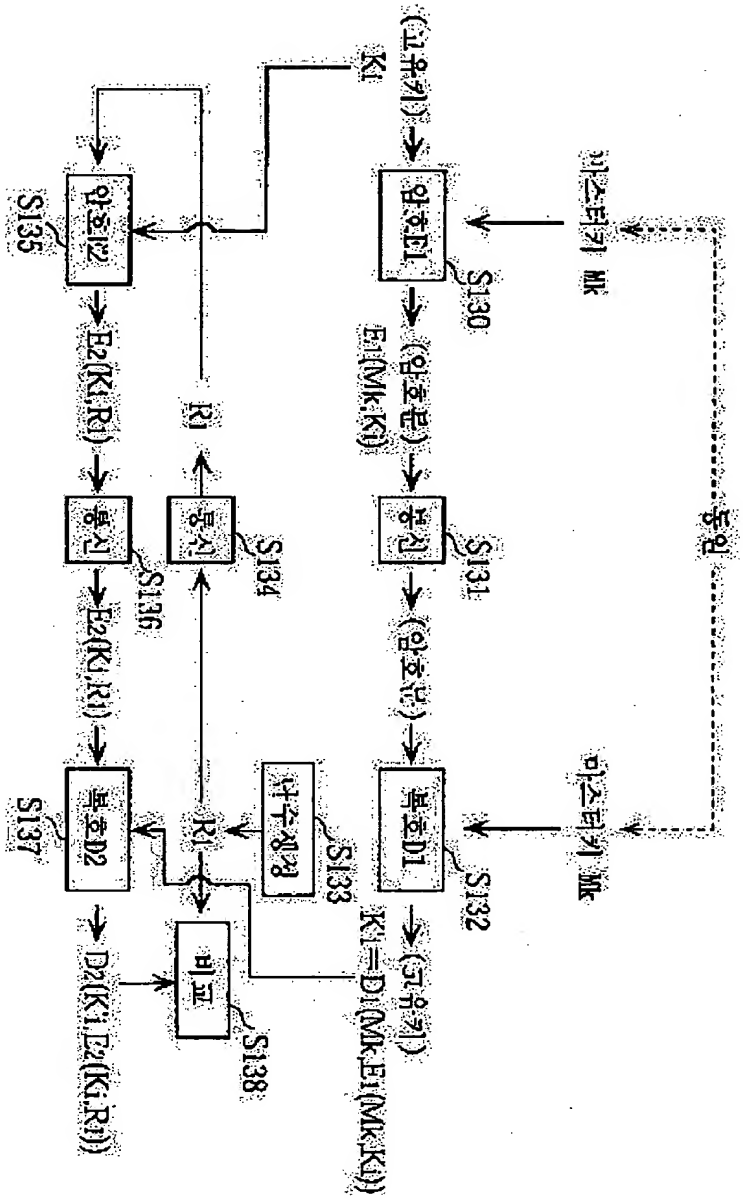
도면8


시작
S120
메모리카드 판독기가 메모리카드를 인증
S121
인증 OK?
아니오
예
S122
메모리카드가 메모리카드 판독기를 인증
S123
인증 OK?
아니오
예
S124
메모리카드는 암호화된 저작물을 메모리카드 판독기로 출력
S125
메모리카드 판독기는 메모리카드로부터 출력된 암호화된 저작물을 복호
S126
메모리카드 판독기는 복호화된 저작물을 재생
종료

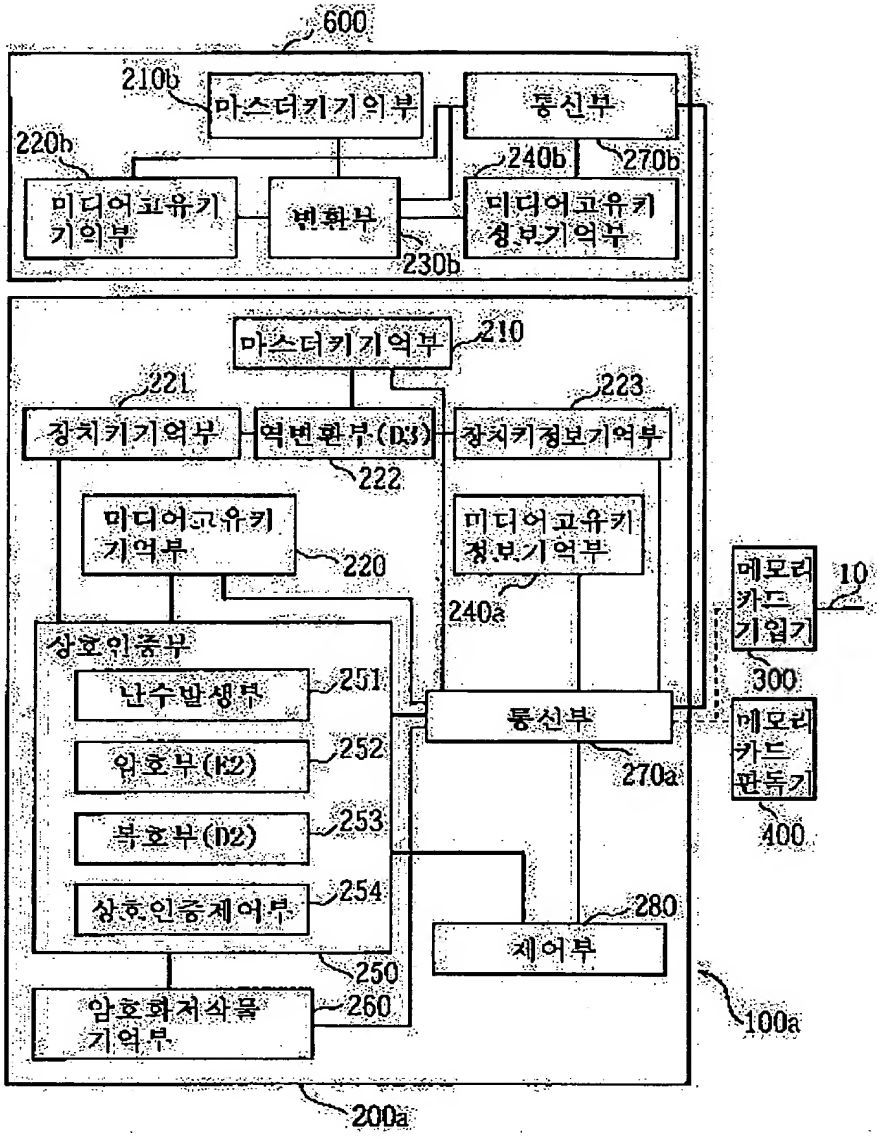
도면9


200
300
E1(Mk,Ki) 생성
S130
E1(Mk,Ki)
S131
S132
K'1←D1(Mk,E1(Mk,Ki))
R1
R1 생성
S133
S134
F2(K1,R1) 생성
S135
F2(K1,R1)
S136
S137
D2(K'1,E2(K1,R1)) 생성
S138
R1:D(K'1,E2(K1,R1)) 비교
E3(Mk,Aj) 생성
S139
S141
E1(Mk,Aj)
S140
A'j←D3(Mk,E3(Mk,Aj))
R2 생성
S142
R2
S143
S144
E2(Aj,R2) 생성
S146
E2(Aj,R2)
S145
D2(A'j,E2(Aj,R2)) 생성
S148
R2:D2(A'j,E2(Aj,R2)) 비교
S147

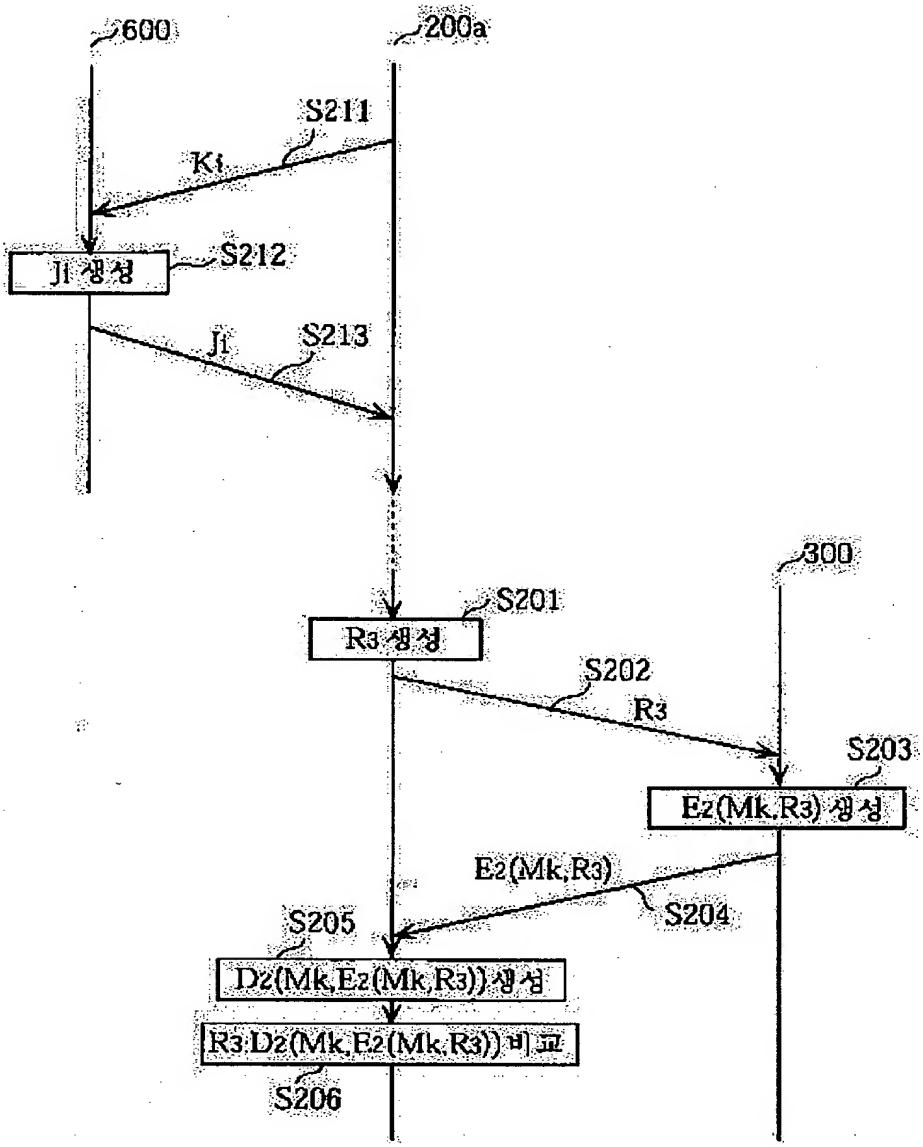
도면10


(고유키)
K1
암호화1
S130
마스터키 Mk
(암호문)
E1(Mk,Ki)
송신
S131
수신
S134
R1
(암호문)
E2(Ki,R1)
암호화2
S135
송신
S136
수신
E2(Ki,R1)
복호화2
S137
R1
난수생성
S133
비교
S138
D2(Ki,E2(Ki,R1))
복호화1
S132
K1=D1(Mk,E1(Mk,K1))
(고유키)
마스터키 Mk
동일

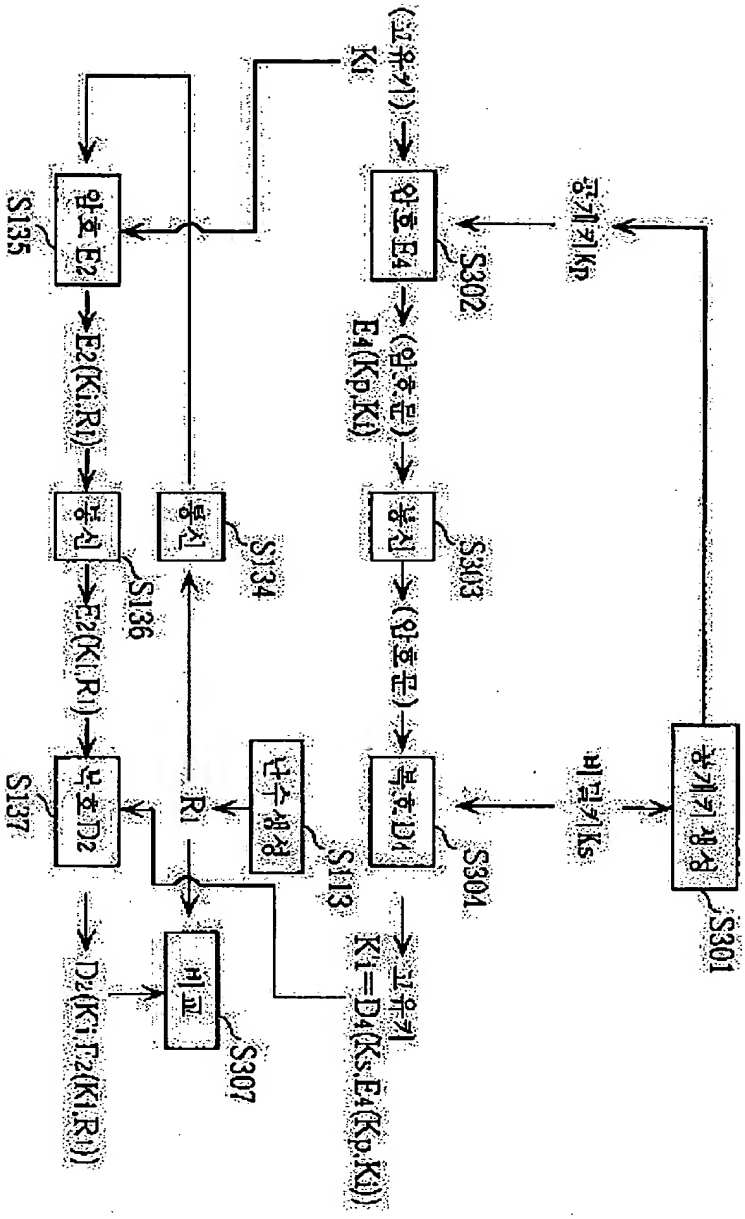
도면1


600
210b
마스터키기억부
통신부
220b
240b
270b
미디어고유키 기억부
변환부
미디어고유키 정보기억부
230b
마스터키기억부
210
221
223
장치키기억부
역변환부(D3)
장치키정보기억부
222
미디어고유키 기억부
220
미디어고유키 정보기억부
240a
메모리 카드 기입기
10
300
상호인증부
난수발생부
251
통신부
메모리 카드 판독기
252
암호부(K2)
270a
400
복호부(D2)
253
상호인증제어부
254
280
제어부
250
암호화처리부 기억부
260
100a
200a

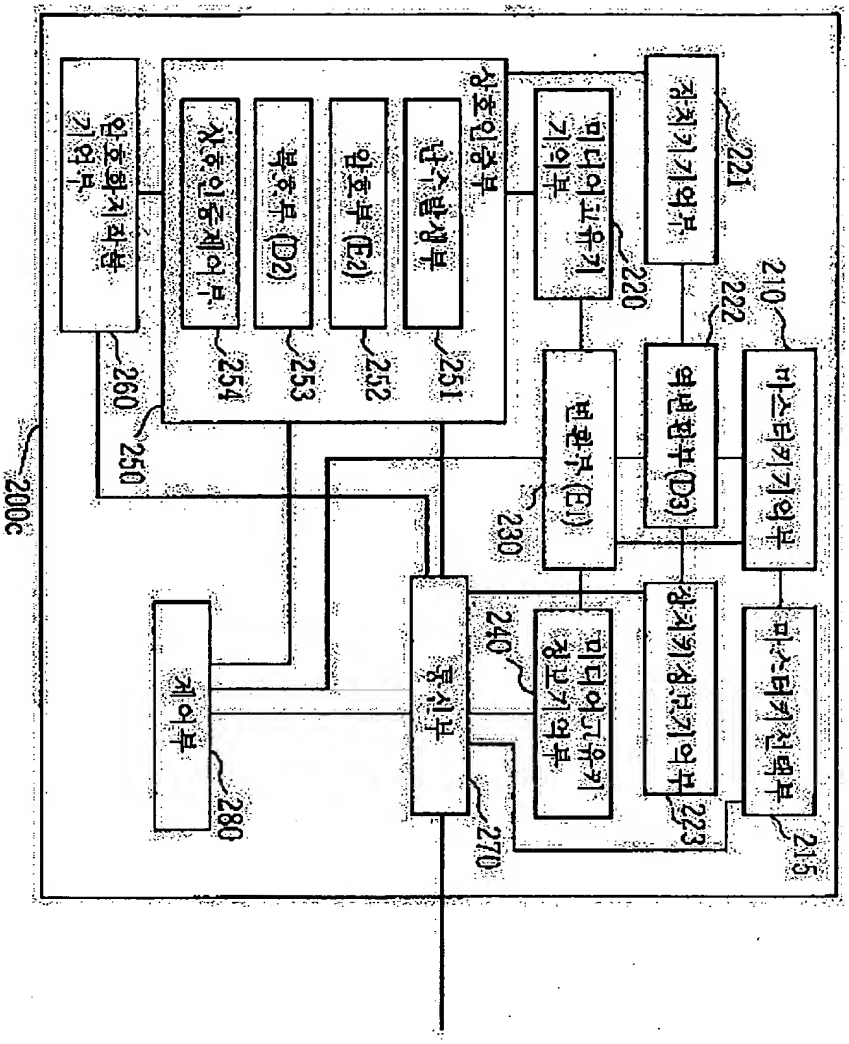
도면12


600
200a
S211
K1
J1 생성
S212
J1
S213
300
S201
R3 생성
S202
R3
S203
E2(Mk,R3) 생성
E2(Mk,R3)
S204
S205
D2(Mk,E2(Mk,R3)) 생성
R3 D2(Mk,E2(Mk,R3)) 비교
S206

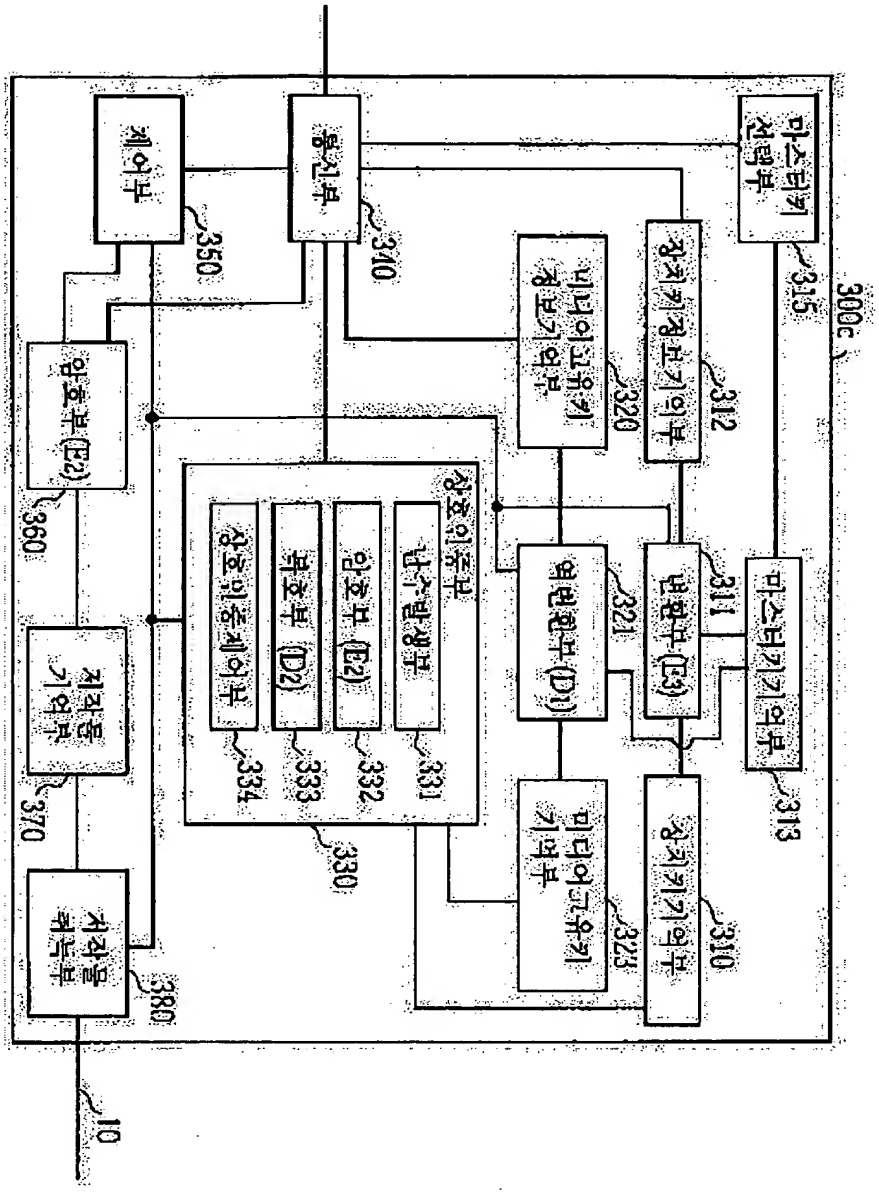
도면13


(고유키) K1
암호 E4
S302
공개키 Kp
E4(Kp,K1)
(암호문)
통신
S303
(암호문)
복호 D1
S301
비밀키 Ks
공개키 생성
S301
K1=D4(Ks,E4(Kp,K1))
고유키
암호 E2
S135
E2(K1,R1)
통신
S136
E2(K1,R1)
복호 D2
S137
통신
S134
난수 생성
S113
R1
비교
S307
D2(K1,E2(K1,R1))

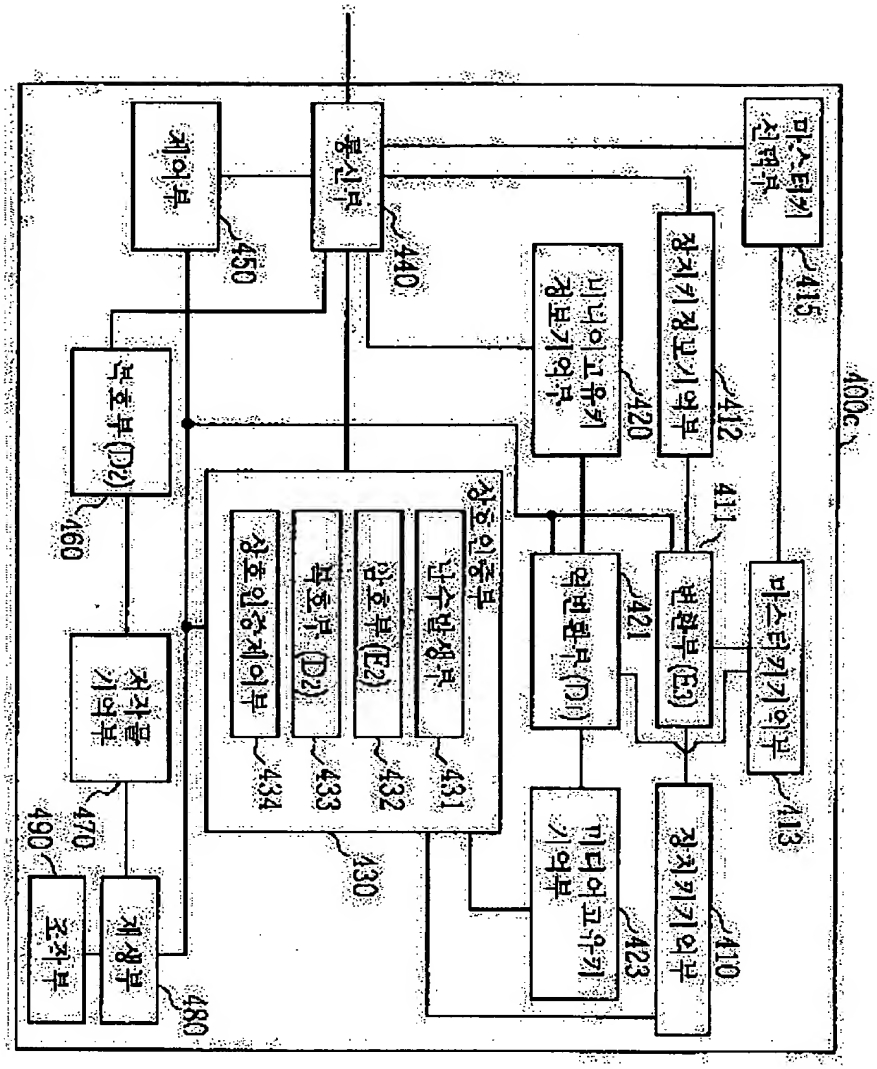
도면14


200c
상호인증부
난수발생부
251
암호부 (E2)
252
복호부 (D2)
253
상호인증제어부
254
암호화키 저장부
260
250
제어부
280
통신부
240
270
변환부 (E1)
230
미디어고유키 저장부
220
역변환부 (D3)
222
210
마스터키 기억부
215
미디어고유키 생성부
223
저치키 기억부
221

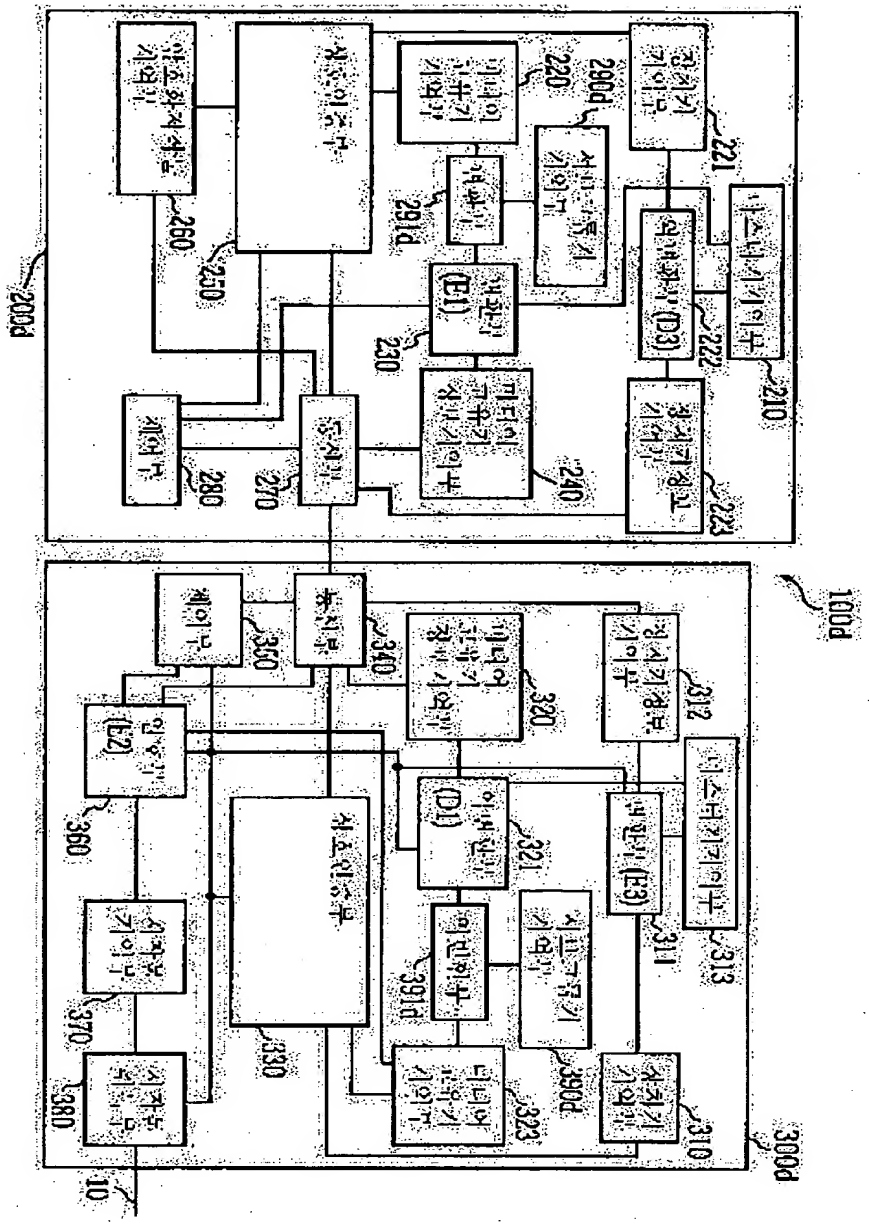
도면15


300c
315
마스터키 선택부
312
장치키정보기억부
320
비닝어고유키 정보기억부
310
통신부
350
제어부
311
변환부 (E3)
321
역변환부 (D1)
313
마스터키기억부
323
비닝어고유키 기억부
310
장치키기억부
330
상호인증부
331
난수발생부
332
암호부 (E2)
333
복호부 (D2)
334
상호인증제어부
360
암호부 (E2)
370
처리물 기억부
380
처리물 취득부
10

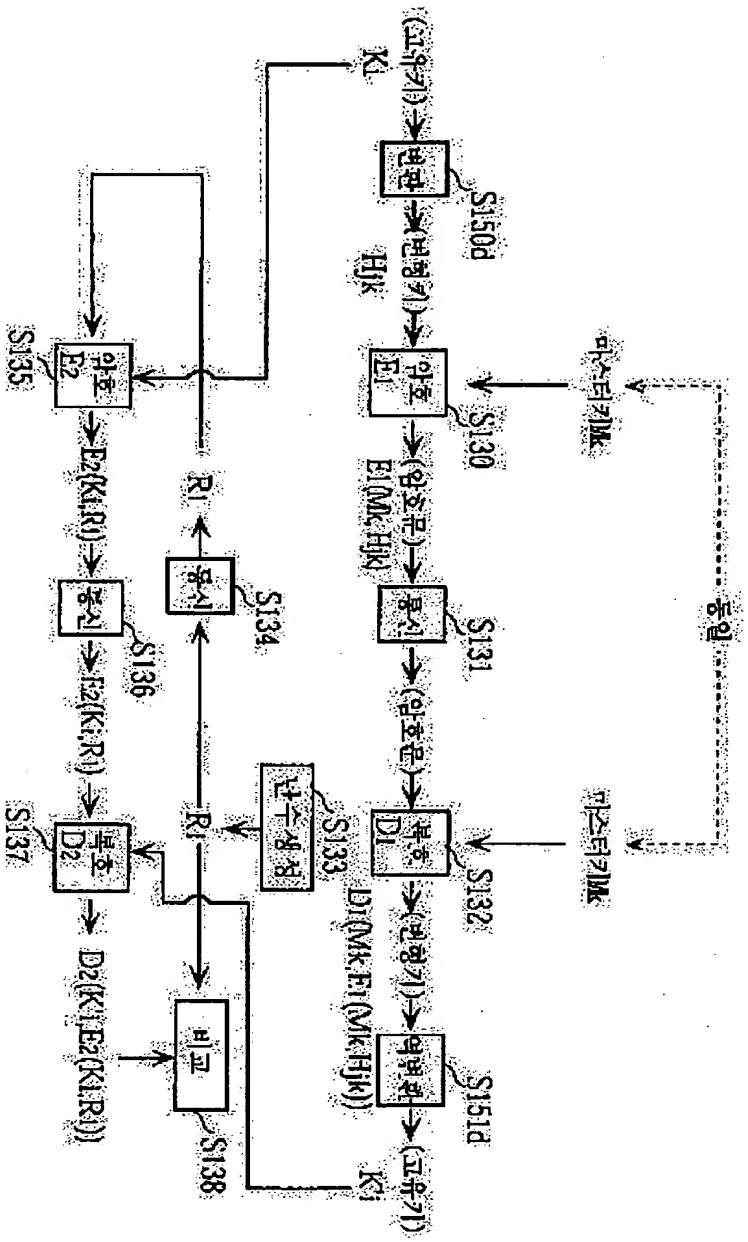
도면8


400c
415
412
420
411
421
410
423
413
440
450
460
430
431
432
433
434
470
490
480
마스터키 선택부
정치키 정보기억부
비터어 고유키 정보기억부
통신부
제어부
복호부(D2)
변환부(E3)
연변환부(D1)
비터어 고유키 기억부
마스터키 기억부
정치키기억부
상호인증부
난수발생부
암호부(E2)
복호부(D2)
상호인증제어부
차량별 키 기억부
제생부
조작부

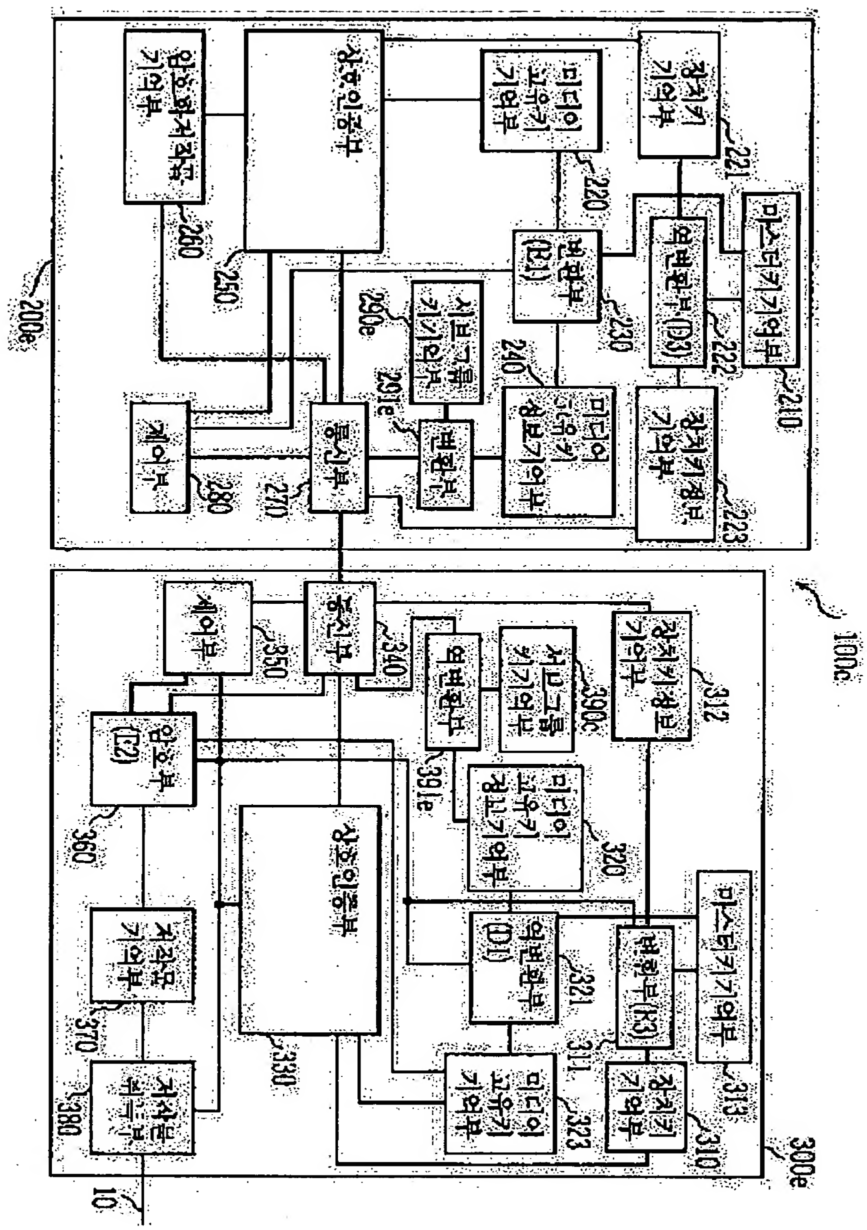
도면17


100d
200d
300d
10
210
220
221
222
223
230
240
250
260
270
280
290d
291d
310
311
312
313
320
321
323
330
340
350
360
370
380
390d
391d
(D1)
(D2)
(D3)
(E1)
(E2)
(E3)

도면18

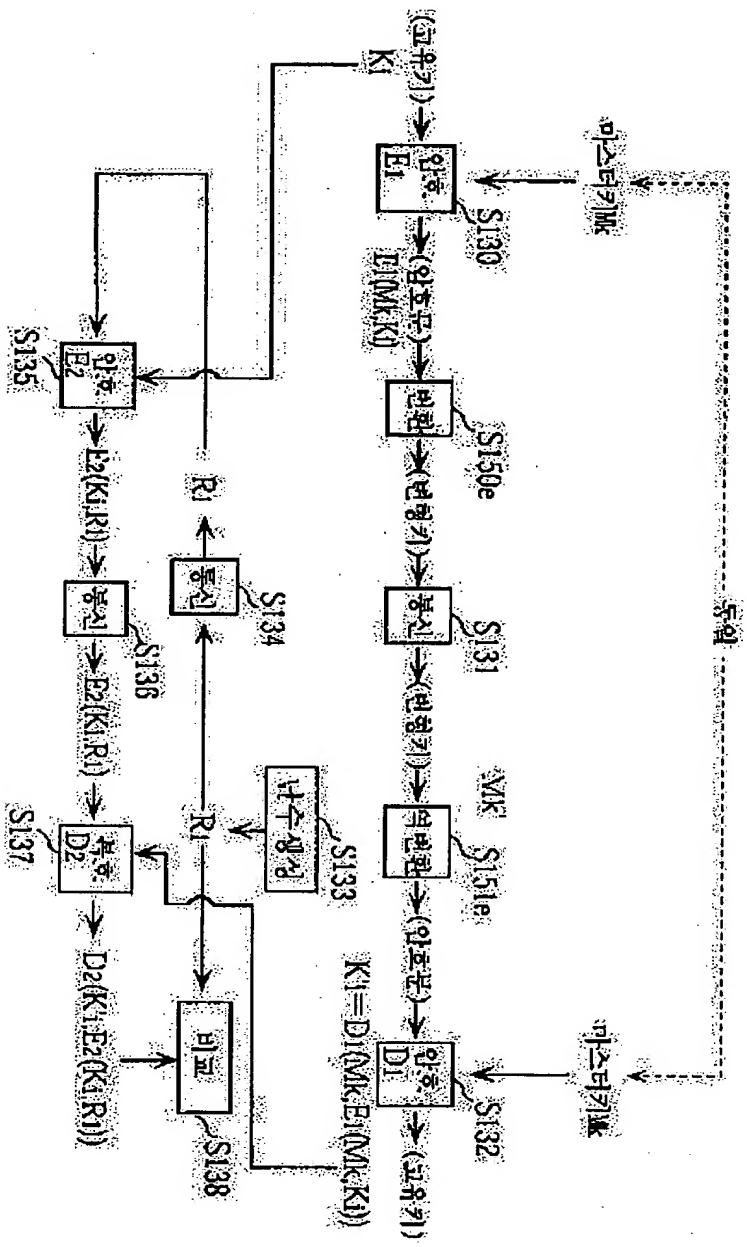

(고유키)
Kj
변환
S150d
(변환키)
Hjk
암호
E1
S130
마스터키Mk
(암호문)
E1(Mk,Hjk)
통신
S131
(암호문)
복호
D1
S132
마스터키Mk
D1(Mk,E1(Mk,Hjk))
(변환키)
역변환
S151d
(고유키)
Kj
난수생성
S133
Ri
통신
S134
Ri
암호
E2
S135
E2(Ki,Ri)
통신
S136
E2(Ki,Ri)
복호
D2
S137
D2(Ki,E2(Ki,Ri))
비교
S138

도면19

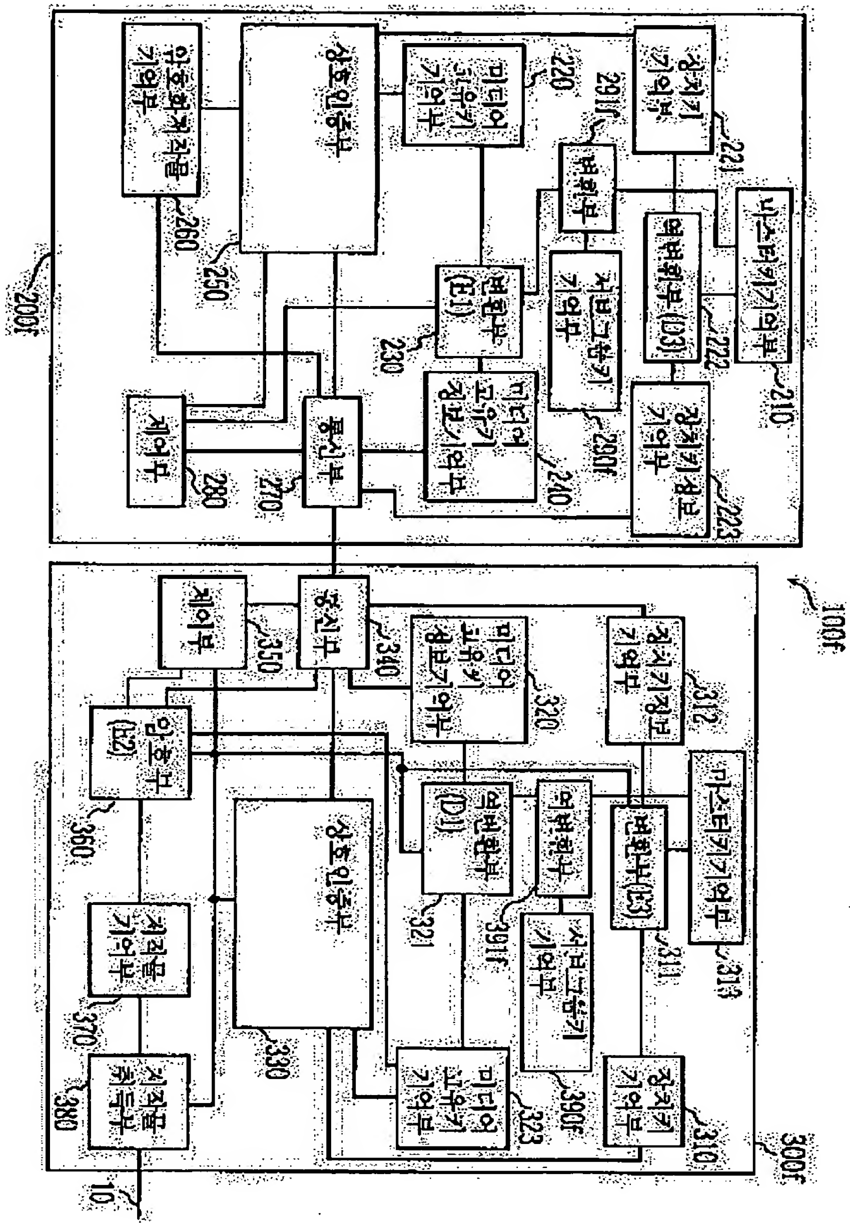


장치키 기억부
221
미디어 고유키 기억부
220
상호인증부
250
암호화저작물 기억부
260
마스터키기억부
210
역변환부(D3)
222
변환부(E1)
230
서브그룹키기억부
290e
미디어 고유키 정보기억부
240
장치키정보 기억부
223
변환부
291e
통신부
270
제어부
280
200e
100e
제어부
350
통신부
340
역변환부
391e
서브그룹키기억부
390e
장치키정보 기억부
312
암호부(E2)
360
미디어 고유키 정보기억부
320
상호인증부
330
역변환부(D1)
321
변환부(E3)
311
마스터키기억부
313
저작물 기억부
370
380
미디어 고유키 기억부
323
장치키 기억부
310
300e
10

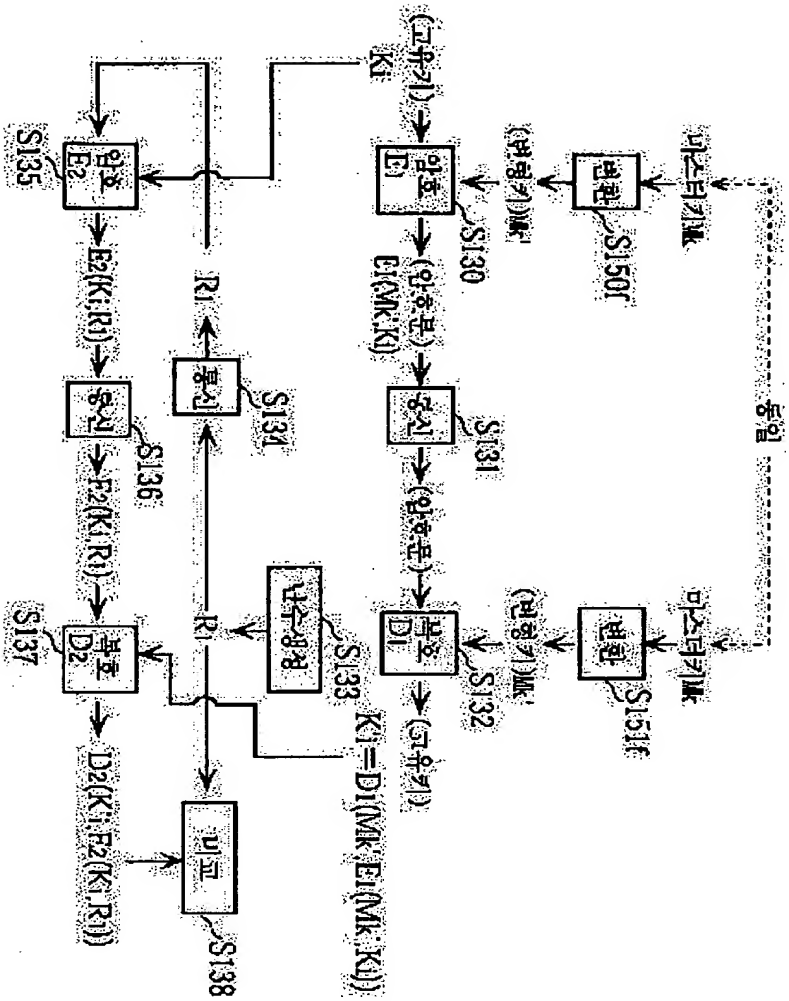
도면20


(고유키)
K1
암호 E1
S130
마스터키
E1(MK,K1)
(암호문)
변환
S150e
(변환키)
복신
S131
(변환키)
VMK
비변환
S151e
(암호문)
K'1=D1(MK,E1(MK,K1))
암호 D1
S132
마스터키
(고유키)
S136
E2(K1,R1)
복호 D2
S137
D2(K1,E2(K1,R1))
비교
S138
R1
통신
S134
R1
난수생성
S133
암호 E2
S135
E2(K1,R1)
통신

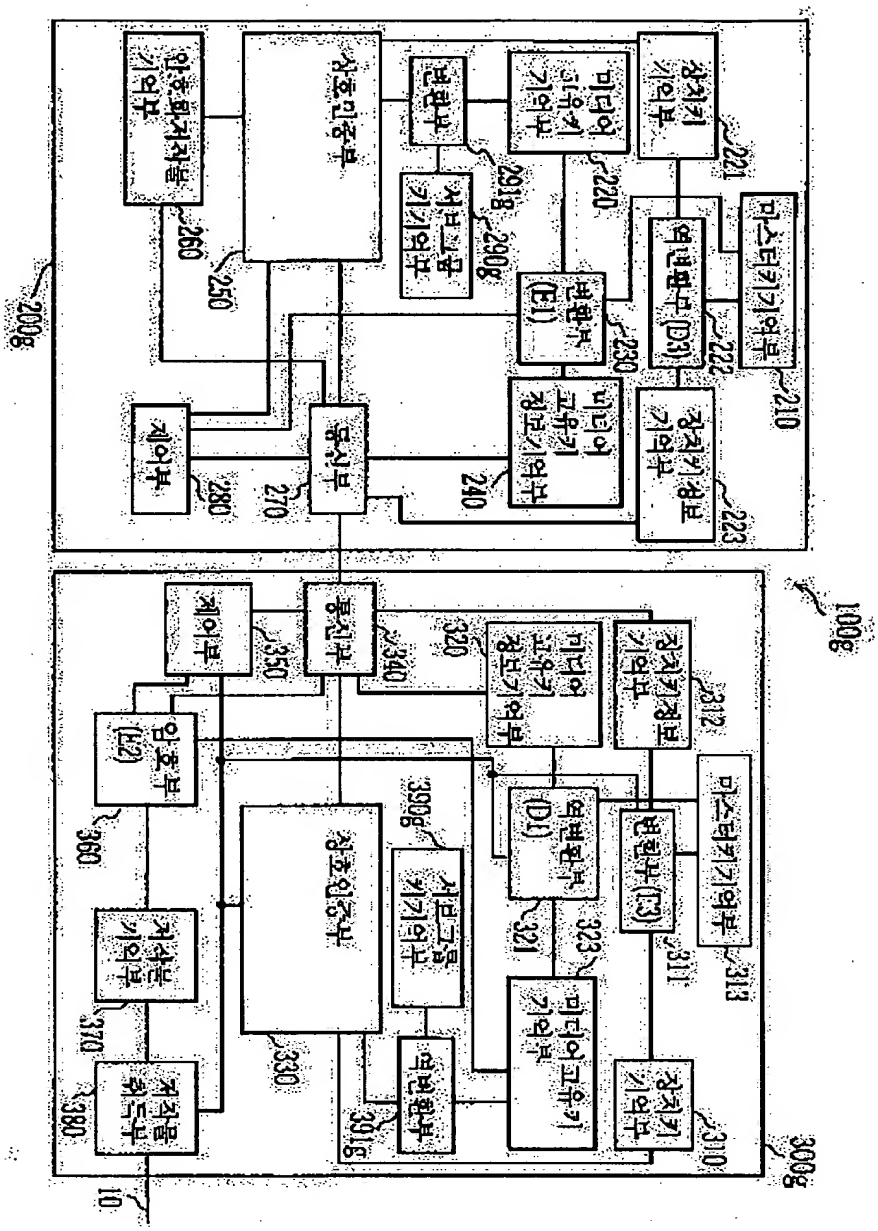
도면21


장치키 기억부
221
마스터키기억부
210
역변환부(D3)
222
장치키정보 기억부
223
291f
변환부
서브그룹키 기억부
290f
미디어 고유키 기억부
220
변환부(E1)
230
미디어 고유키 정보기억부
240
상호인증부
250
암호화저작물 기억부
260
통신부
270
제어부
280
200f
100f
제어부
350
통신부
340
미디어 고유키 정보기억부
320
장치키정보 기억부
312
마스터키기억부
313
변환부(E3)
311
역변환부
391f
역변환부(D1)
321
서브그룹키 기억부
390f
장치키 기억부
310
미디어 고유키 기억부
323
상호인증부
330
암호부(E2)
360
저작물 기억부
370
저작물 취득부
380
10
300f

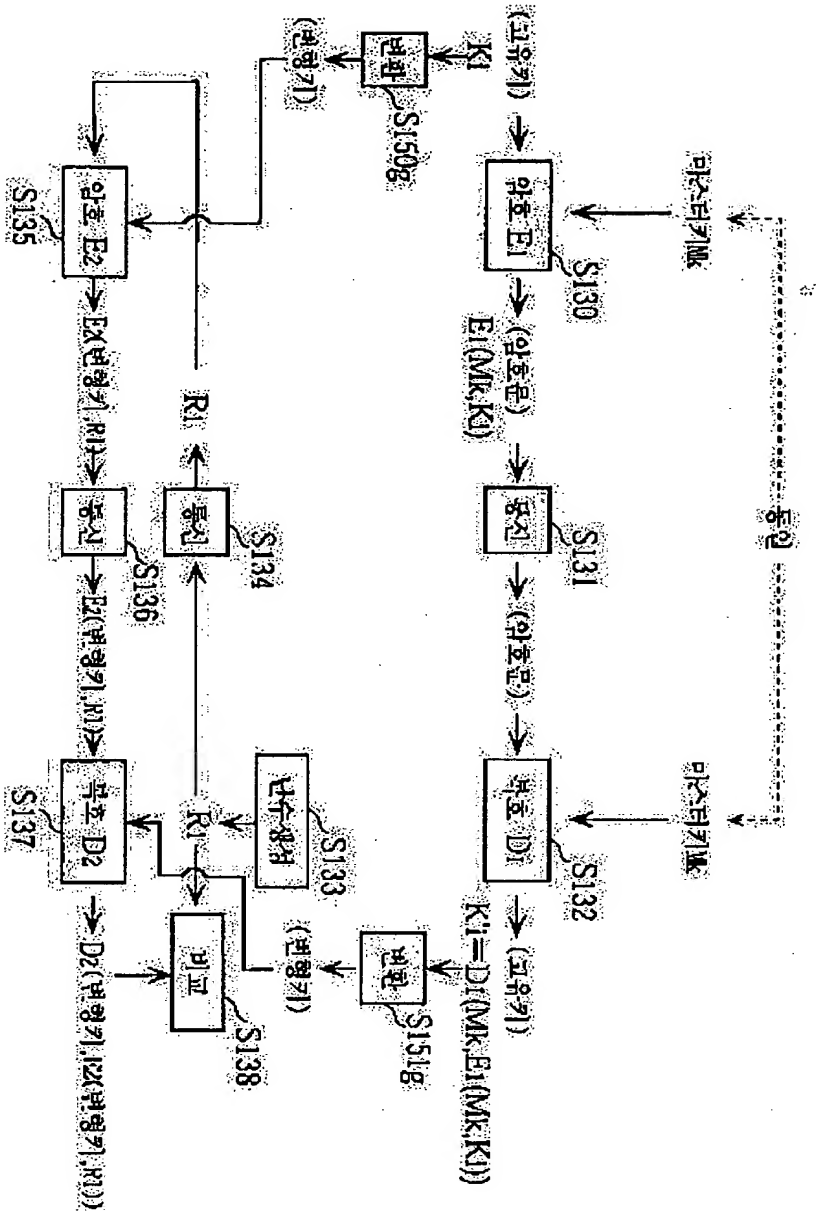
도면22


마스터키Mk
동일
변환
S150
(변형키)Mk'
암호
E1
S130
(고유키)
Ki
E1(Mk;Ki)
연산
S131
(암호문)
복호
D1
S132
(변형키)Mk'
변환
S151
마스터키Mk
(고유키)
Ki=D1(Mk';E1(Mk;Ki))
난수생성
S133
Ri
홍신
S134
암호
E2
S135
E2(Ki;Ri)
연산
S136
F2(Ki;Ri)
복호
D2
S137
D2(Ki;F2(Ki;Ri))
비교
S138

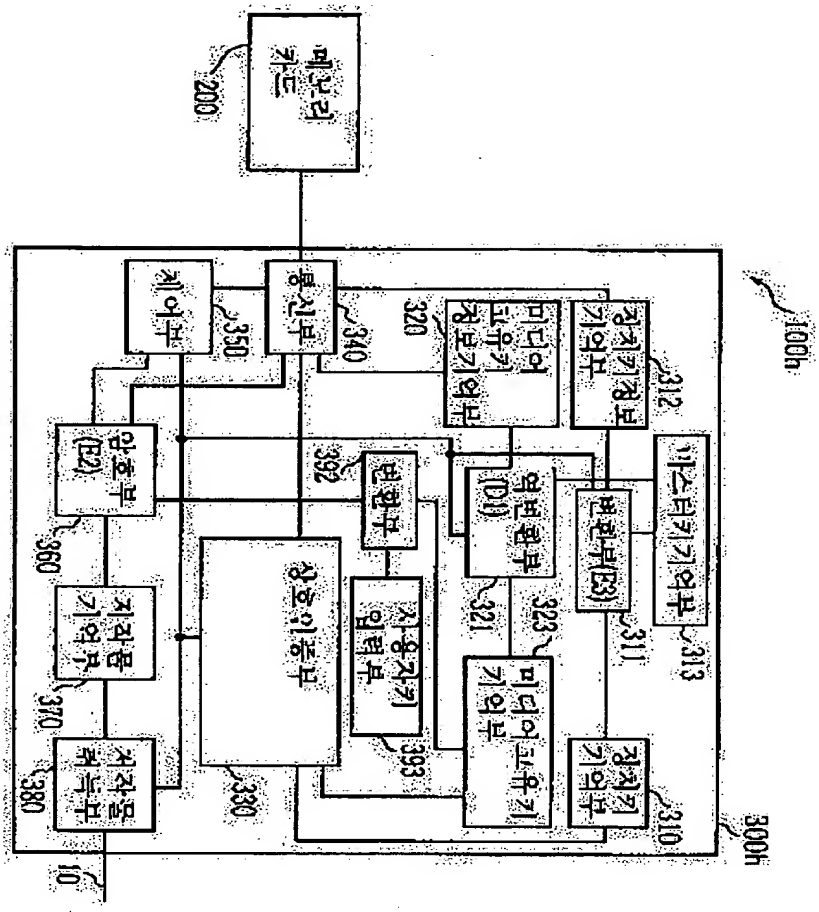
도면23


100g
200g
300g
10
210
220
221
222
223
230
240
250
260
270
280
290g
291g
310
311
312
313
320
321
323
330
340
350
360
370
380
390g
391g
D1
D2
D3
E1
E2
마스터키억부
상치키 기억부
역변환부 (D3)
변환부 (E1)
미더어 고유키 정보기억부
상치키정보 기억부
서브그룹 키기억부
변환부
미더어 고유키 기억부
상호인증부
인증 패러자불 기억부
제어부
동신부
암호부 (E2)
제어부
통신부
미더어 고유키 정보기억부
상치키 기억부
역변환부 (D1)
변환부 (E1)
마스터키억부
상치키정보 기억부
미더어 고유키 기억부
서브그룹 키기억부
상호인증부
암호부 (E2)
키생성부
키저장 메모리부

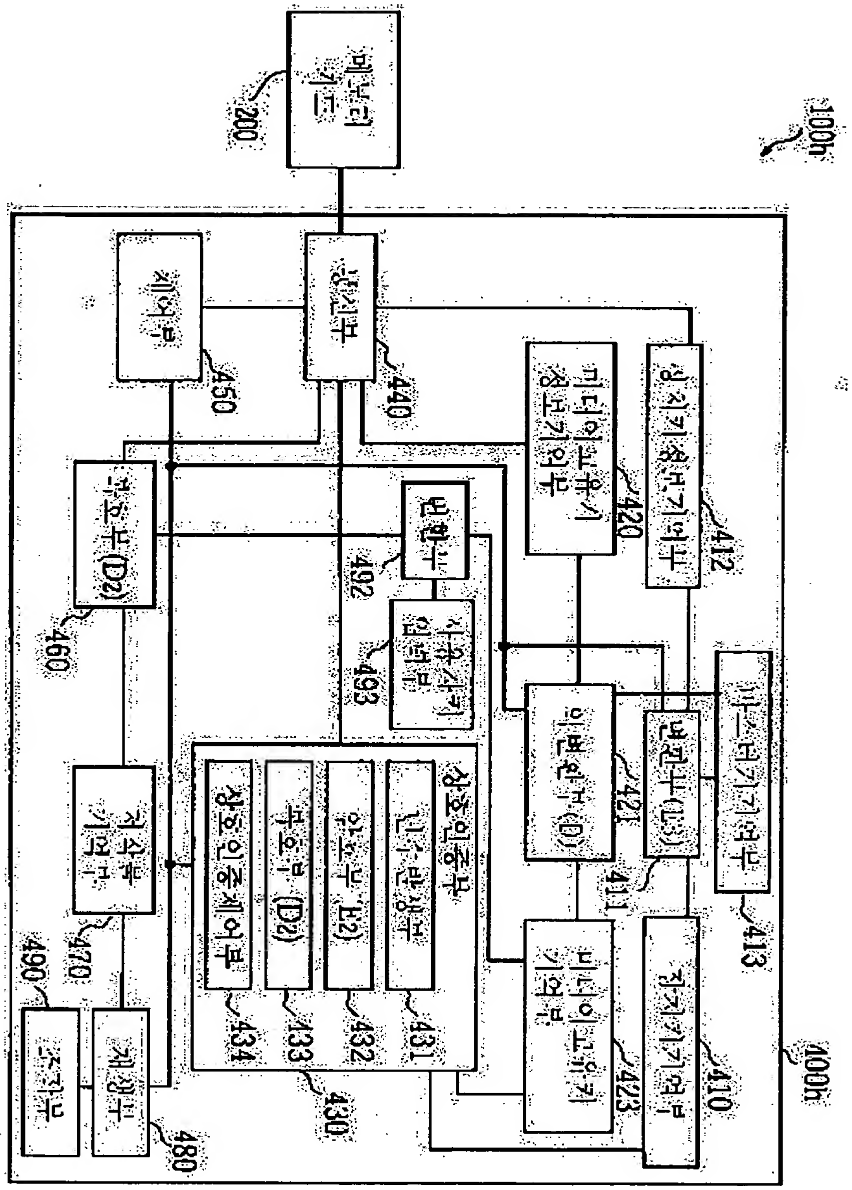
도면24


마스터키K
암호 E1
S130
E1(MK,KJ)
(암호문)
통신
S131
(암호문)
복호 D1
S132
KJ'=D1(MK,E1(MK,KJ))
(고유키)
변환
S151g
(변형키)
난수생성
S133
RJ
비교
S138
D2(변형키,E2(변형키,RJ))
복호 D2
S137
E2(변형키,RJ)
통신
S136
RJ
통신
S134
EX(변형키,RJ)
암호 E2
S135
(변형키)
변환
S150g
KJ
(고유키)
마스터키K
동일

도면25


메모리 카드
200
통신부
340
체어부
350
암호부 (B2)
360
저작물 기억부
370
저작물 처분부
380
상호인증부
330
변환부
392
사용자키 입력부
393
미디어 고유키 저장기억부
320
웹브라우저 (B1)
321
미디어 고유키 기억부
323
변환부(B3)
311
비즈터키기억부
313
장치키정보 기억부
312
장치키 기억부
310
100h
300h
10

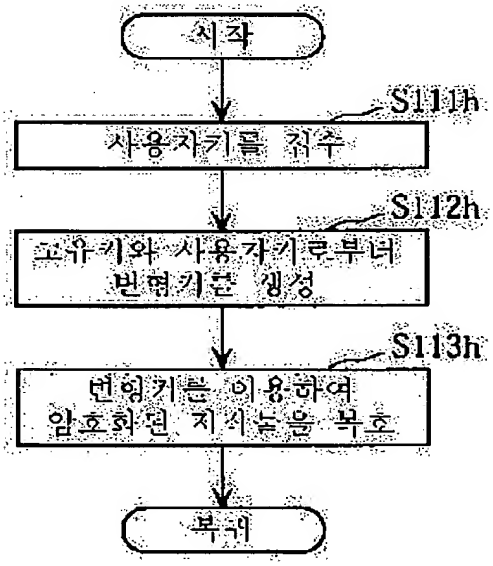
도면28


100h
메모리 카드
200
400h
413
412
410
420
421
411
423
440
제어부
450
변환부
492
493
상호인증부
431
432
433
434
430
복호부(D2)
460
470
재생부
480
조작부
490

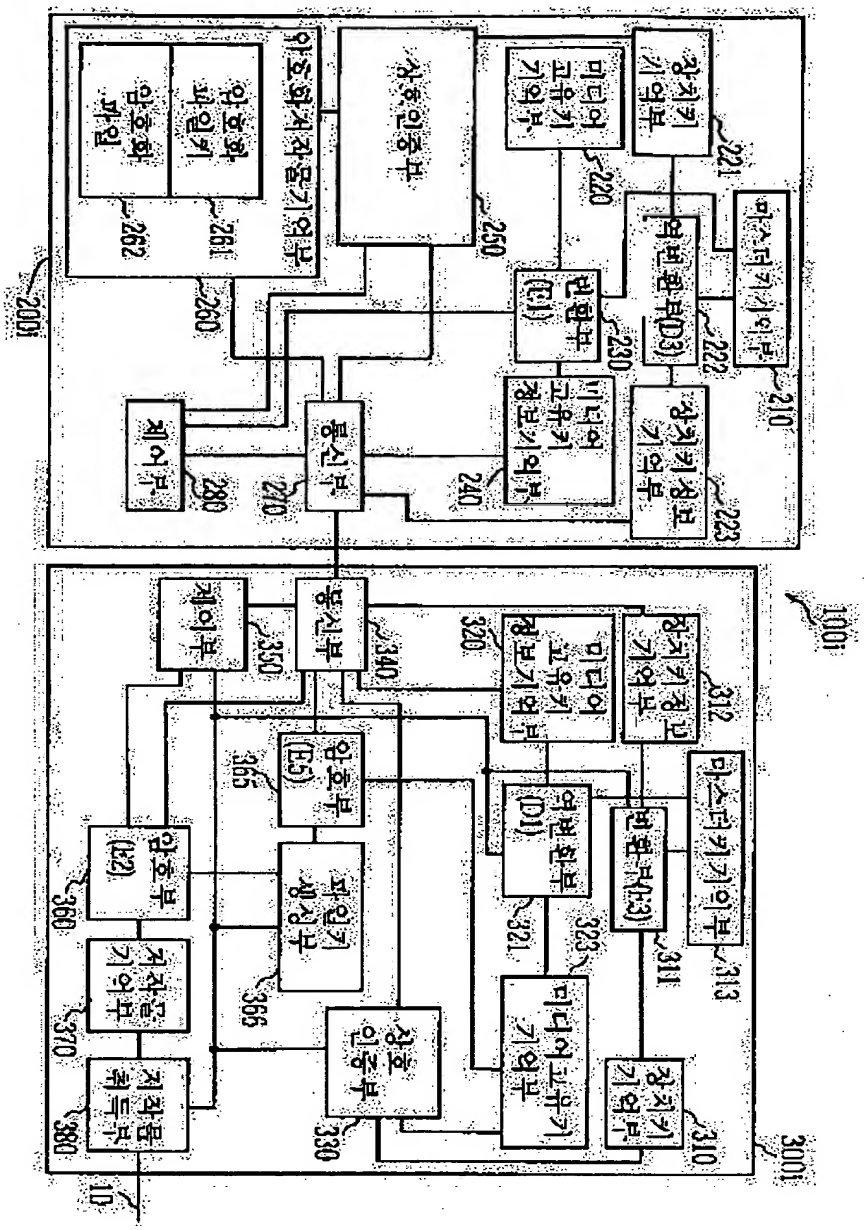
도면27


시작
S100h
사용자키를 입수
S101h
고유키와 사용자키로부터
변형키를 생성
S102h
변형키를 이용하여 처리물을
암호화
S103h
암호화된 처리물을
메모리카드로 출력
복귀

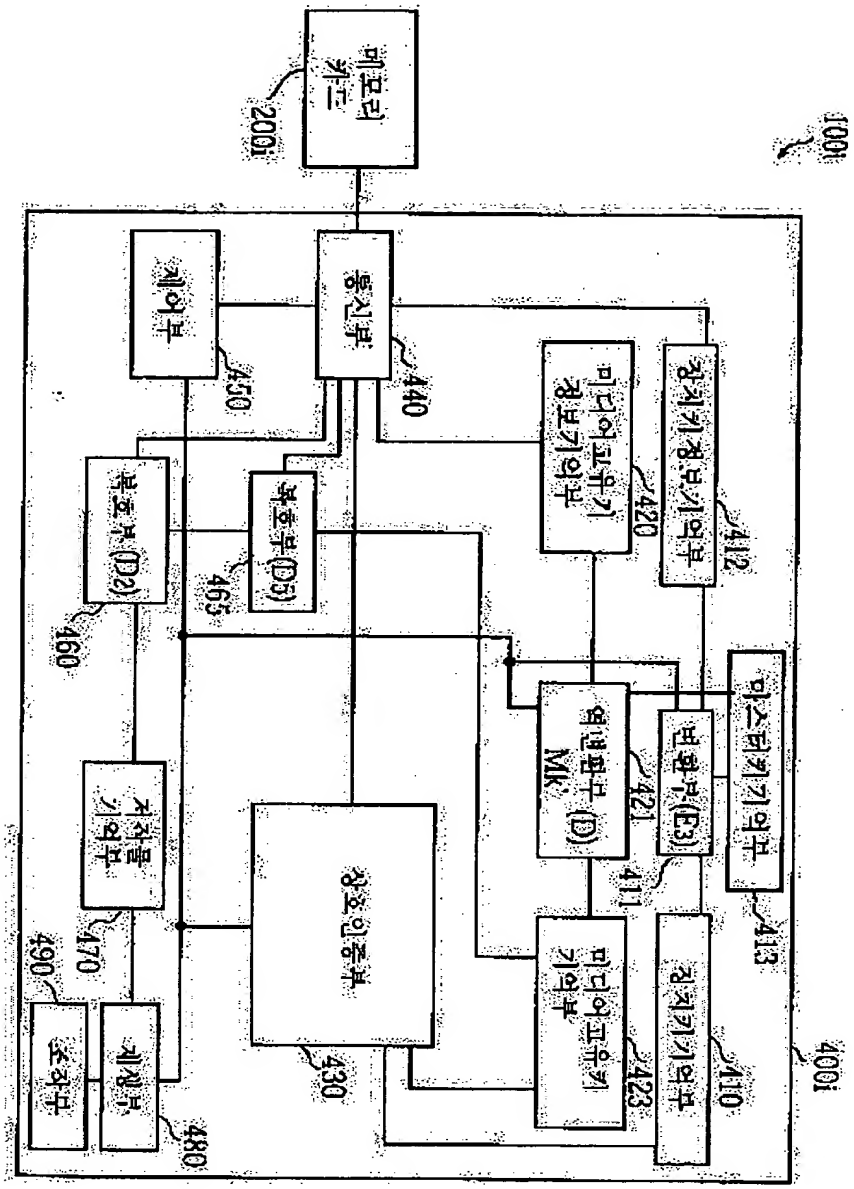
도면28


시작
S111h
사용자키를 입수
S112h
고유키와 사용자키로부터
변형키를 생성
S113h
변형키를 이용하여
암호화된 처리물을 복호
복귀

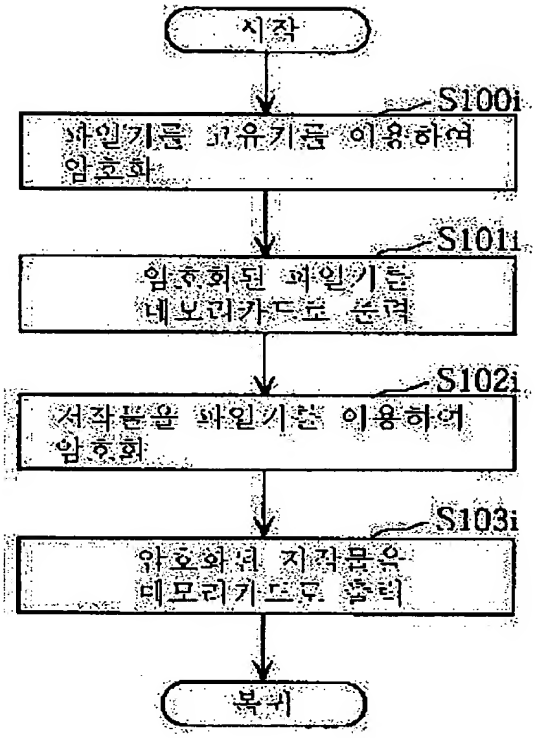
도면29


100i
200i
210
마스터 키 인부
221
장치키 인식부
220
미디어 고유키 인식부
222
변복원부(D3)
230
변복부(D1)
240
상치키정보 기억부
223
상호인증부
250
암호화 파일키
261
암호화 파일
262
암호화처리정보기억부
260
체어부
280
통신부
270
3001
310
장치키 기억부
311
마스터키 기억부
313
변복부(D3)
321
변복원부(D1)
323
미디어 고유키 정보기억부
320
장치키정보 기억부
312
미디어 고유키 인식부
340
통신부
350
체어부
암호부(E5)
365
암호부(E2)
360
파일키 생성부
366
차량별 키 인부
370
차량별 키 취득부
380
상호 인증부
330
10

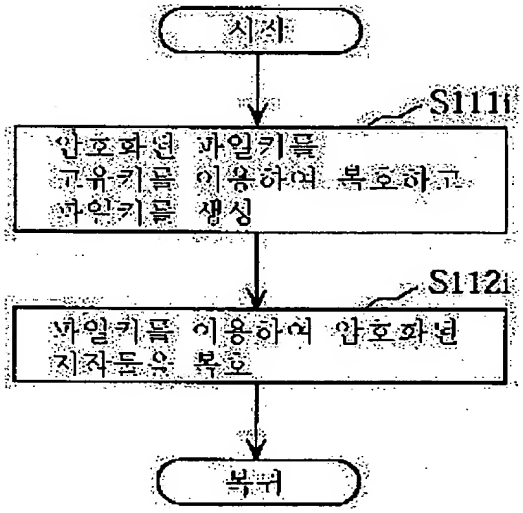
도면30


메모리 카드
200
1001
통신부
440
제어부
450
복호부(D2)
460
복호부(D5)
465
처리물 기억부
470
조작부
490
게임부
480
정치정보기억부
412
미디어고유키 정보기억부
420
암호화부 (D) Mk
421
변환부(E3)
411
마스터키기억부
413
정치키기억부
410
미디어고유키 기억부
423
상호인증부
430
400i

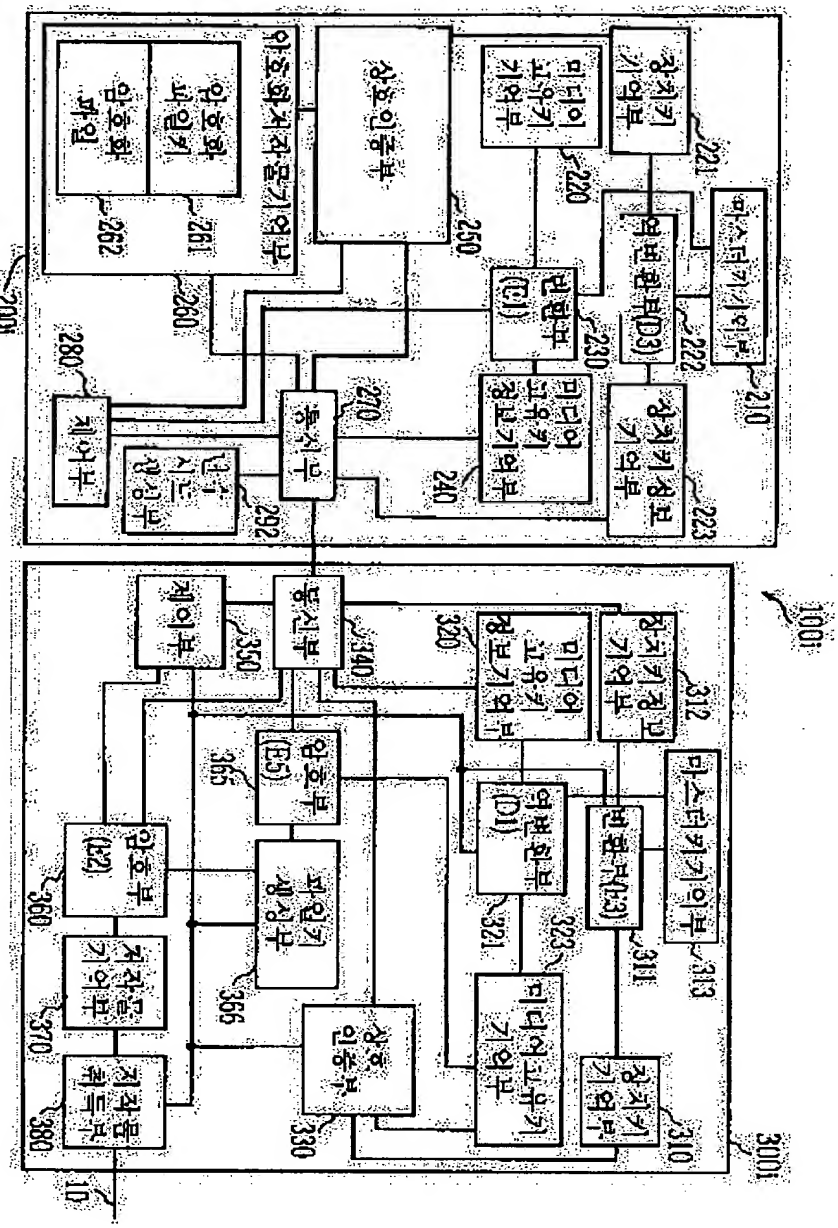
도면31


시작
S100i
파일키를 고유키를 이용하여 암호화
S101i
암호화된 파일키를 메모리카드로 전송
S102i
저작물을 파일키를 이용하여 암호화
S103i
암호화된 저작물을 메모리카드로 출력
복귀

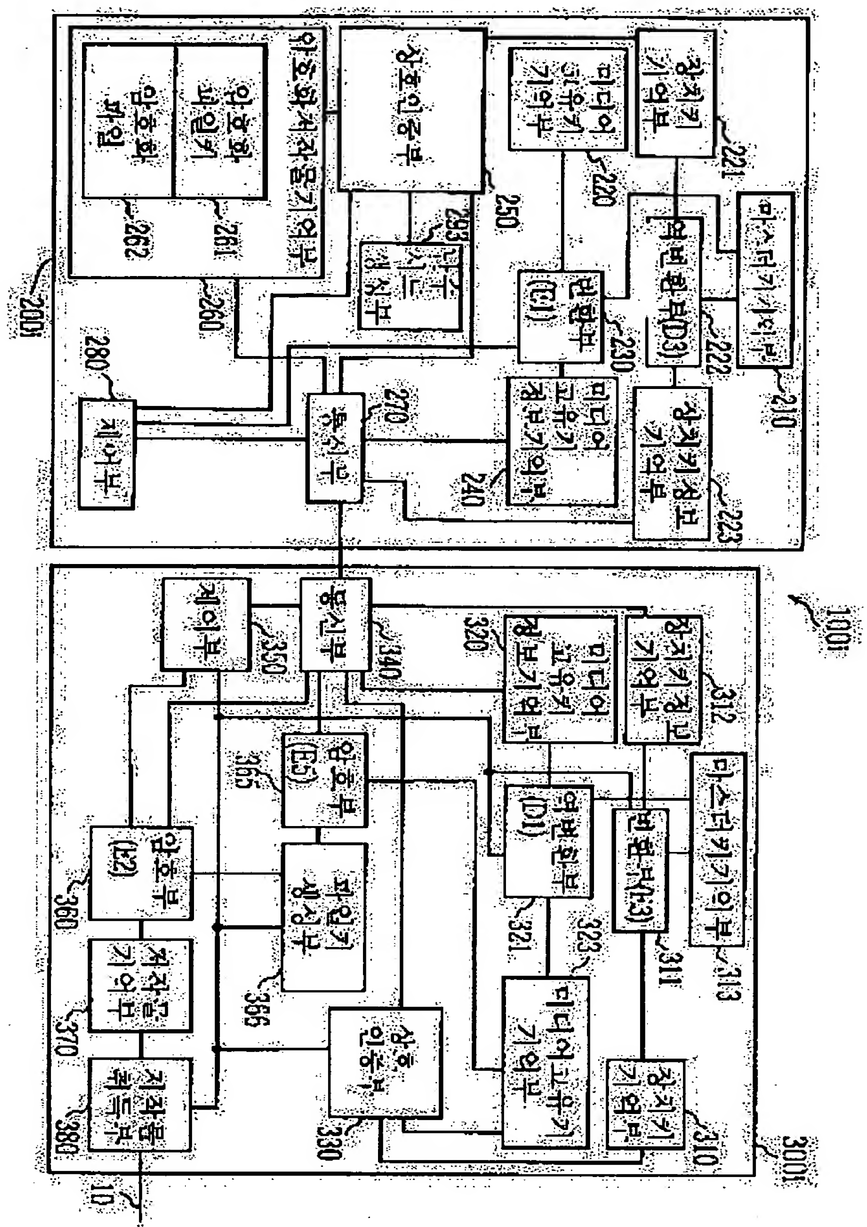
도면32


시작
S111i
암호화된 파일키를 고유키를 이용하여 복호하고 파일키를 생성
S112i
파일키를 이용하여 암호화된 저작물을 복호
복귀

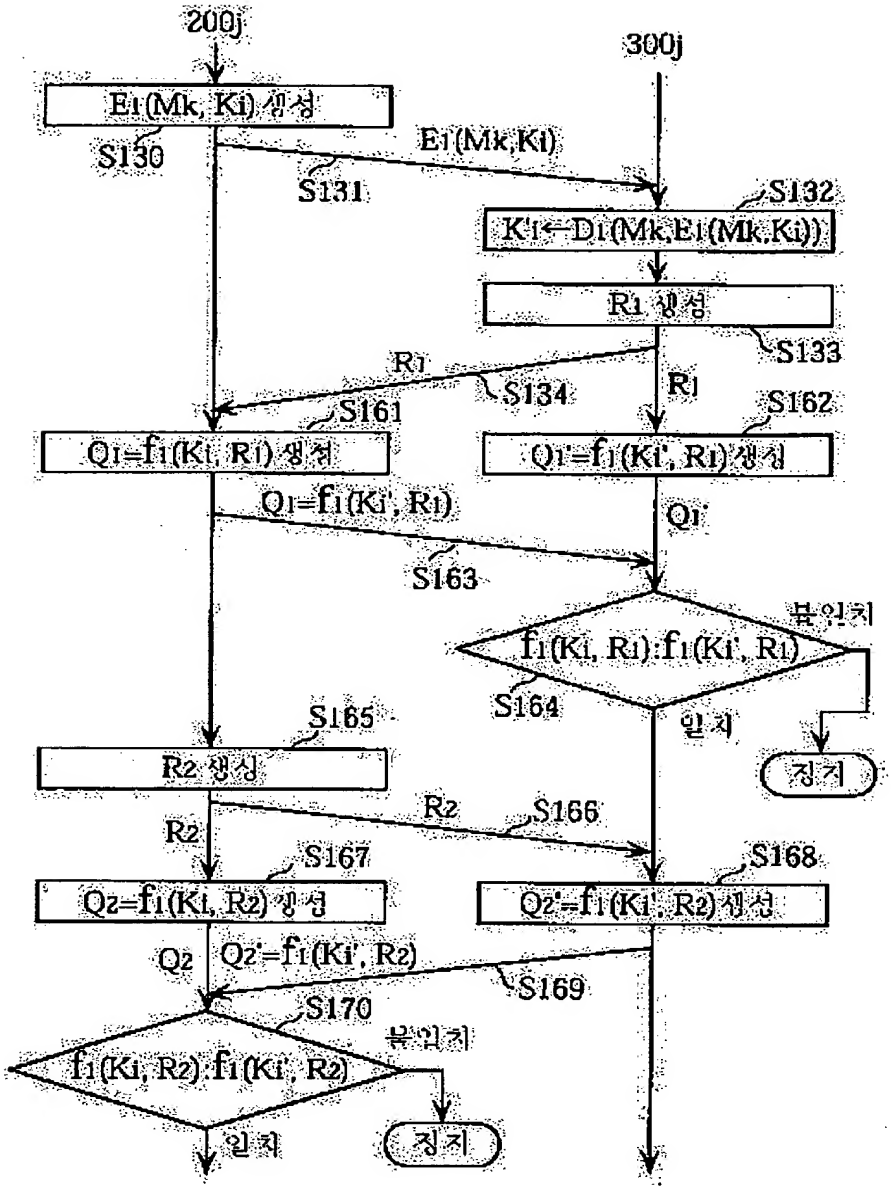
도면33


100
200
210 마스터키 입부
220 미디어 고유키 기억부
221 장치키 기억부
222 변환부(D3)
223 상치키정보 기억부
230 변환부 (D1)
240 미디어 고유키 정보기억부
250 상호인증부
260 암호화처리용기억부
261 암호화 파일키
262 암호화 파일
270 통신부
280 제어부
292 난수 생성부
300
310 장치키 기억부
311 변환부(D3)
312 장치키정보 기억부
313 마스터키입부
320 미디어 고유키 정보기억부
321 변환부 (D1)
323 미디어고유키 기억부
330 상호 인증부
340 통신부
350 제어부
365 암호부 (E5)
366 파일키 생성부
368 암호부 (E2)
370 처리용 기억부
380 처리용 취득부
10

도면34


장치키 기억부
221
미디어 고유키 기억부
220
상호인증부
250
암호화저작물기억부
암호화 파일키
261
암호화 파일
262
260
마스터키기억부
210
역변환부(D3)
222
변환부(E1)
230
시드 생성부
293
장치키정보 기억부
223
미디어고유키 정보기억부
240
통신부
270
제어부
280
2001
1001
통신부
340
제어부
350
미디어 고유키 정보기억부
320
장치키정보 기억부
312
마스터키기억부
313
변환부(E3)
311
역변환부(D1)
321
암호부(E5)
365
파일키 생성부
366
암호부(E2)
360
저작물 기억부
370
저작물 취득부
380
상호인증부
330
미디어고유키 기억부
323
장치키 기억부
310
3001
10

도면35


200j
300j
E1(Mk, Ki) 생성
S130
E1(Mk,Ki)
S131
S132
K'i←D1(Mk,E1(Mk,Ki))
R1 생성
S133
R1
S134
R1
S161
S162
Q1=f1(Ki, R1) 생성
Q1'=f1(Ki', R1) 생성
Q1=f1(Ki', R1)
Q1'
S163
f1(Ki, R1):f1(Ki', R1)
S164
불일치
일치
정지
S165
R2 생성
R2
S166
R2
S167
S168
Q2=f1(Ki, R2) 생성
Q2'=f1(Ki', R2) 생성
Q2
Q2'=f1(Ki', R2)
S169
S170
f1(Ki, R2):f1(Ki', R2)
불일치
일치
정지

This Page is Inserted by IFW Indexing and Scanning Operations and is not part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☑ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☑ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☑ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.
As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.